DEFENSE INNOVATION BOARD

BUILDING A DOD DATA ECONOMY

DIB DEFENSE INNOVATION BOARD
innovation.defense.gov

Table of Contents

Preface

As an organization, the Department of Defense (DoD) has fallen far behind in modeling data-centricity and facilitating data access. Industry has outpaced us by decades, incorporating data management principles across the entire lifecycle. Today, first-rate companies demand interoperability within their software; within DoD, organizations remain riddled with systems that are incapable of data integration via Application Programming Interfaces (APIs).

Some parts of DoD have begun to incorporate modern data practices into their routine operations, but the majority of Components are failing to provide a unified approach to managing data access, sharing, and use. Data interoperability is not simply a matter of technological convenience, it is a critical underpinning of long-term operational effectiveness, and thus a strategic imperative for maintaining DoD's tradition of warfighting excellence in an increasingly data-centric global environment.

The Defense Innovation Board (DIB) is chartered with the authority and responsibility to provide independent, practical, and actionable recommendations to the Secretary of Defense and other DoD leaders on catalyzing innovation within the Department to strengthen our national security and warfighting capabilities. Today, DoD's ability to counter threats to national security wholly depends on informed decision-making from the boardroom to the battlefield. This study, with its initial focus on data access in collaboration with industry, will meaningfully address that mission.

The following DIB report underscores the need to address, in short order, the fundamental cornerstone of any modern data economy: streamlined data access through immediate improvements in data interoperability across the defense innovation ecosystem, as well as longer-term changes for eroding entrenched data silos and empowering communities of young digital natives to thrive. The driving, underlying assumption of these suggested actions is that failure to adopt data best practices will degrade the force and leave our nation unprepared for future conflicts. The DIB's recommendations, taken as a whole, offer a roadmap to meaningfully advance DoD efforts to unleash the Department's data-as-a-product strategy and establish a robust data economy by 2025.

This study reflects the passion and commitment of the Defense Innovation Board members to drive change and scale innovation at the Department in support of our national defense mission. Their findings are supported by a rigorous research approach triangulating academic insights, industry practice, and Department of Defense context and equities from across the services.

Acknowledgements

Defense Innovation Board Members

Michael R. Bloomberg, Chair
Ryan Swann
Dr. Gilda Barabino
Mary Meeker
Hon. Dr. Will Roper
with
Hon. Sue Gordon
Reid Hoffman
Admiral (Ret.) Mike Mullen
Charles Phillips
Hon. Mac Thornberry

Executive Director

Dr. Marina Theodotou

Staff

Jacob Sharpe
Elliot Silverberg

Khalia Alexander
Zackariah Crahen
Logan Hatfield
Melanie Heinlein
Christina Hilf
Abigail Linman
Dr. Juan Merizalde

Executive Summary

The Defense Innovation Board (DIB) was tasked to deliver a study that provides outcomes-driven recommendations on how to build and scale the Pentagon's data economy.[1] According to the *Massachusetts Institute of Technology (MIT) Technology Review*, a data economy comprises "the global digital ecosystem in which the producers and consumers of data …can glean richer business insights, tap into unexplored markets, serve citizens and consumers alike with data-driven products and services, and monetize their data by sharing it externally with key customers and suppliers."[2] A thriving Department of Defense (DoD) data economy is an essential toolset for a more networked future and current force. Properly constructed, this data economy will transform the defense landscape and ensure U.S. national security in the 21st century.

To evaluate the current maturity of the DoD data economy, the DIB convened discussions across the entire DoD data ecosystem to identify pragmatic insights, best practices, and solutions to specific challenges. In the process, we found that:

- Data innovation is happening in vertical silos, and data access remains *the* central enterprise-level obstacle to the sharing and use of data for the warfighter.
- Past data strategies and the Deputy Secretary's "data decrees" have proven difficult to operationalize and scale across DoD Components owing to unfocused implementation.[3]
- The DoD Chief Digital and Artificial Intelligence Officer (CDAO) is an important entity but faces challenges in establishing itself as *the* DoD data economy leader.
- Absent focused leadership, the Military Departments (MILDEPs) and Combatant Commands (COCOMs) are haphazardly hiring, placing, and utilizing their data leaders.
- DoD is not empowering its young digital natives, upskilling its workforce, and attracting new data talent with sufficient speed.
- Despite talking about the importance of data, DoD programs rarely reward it contractually. In many cases, the open-systems approach simply equates to lost revenue for defense contractors. This stands in stark contrast to commercial industries who successfully monetize access to and exploitation of data produced by their platforms.
- Data-related initiatives lack a substantial, multi-year, topline budgetary allocation that clarifies and sustains the financial incentive for industry to engage the DoD data economy.

The throughline of these identified challenges is data access, which drives this study's overarching recommendation that in order to build a robust data economy, DoD must first address its lack of seamless data extensibility and interoperability through a unified, scalable data access approach.[4] Data has always been a critical strategic asset in success. It is becoming more so by the

[1] Department of Defense, Deputy Under Secretary of Defense for Research and Engineering (2023, October 10), *Terms of Reference - Building a DoD Data Economy*

[2] MIT Technology Review Insights (2023, September 15). *Capitalizing on the data economy*. MIT Technology Review. https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/

[3] Department of Defense, Deputy Secretary of Defense (2021, May 5), *Creating Data Advantage*

[4] Stakeholders most frequently emphasized challenges with accessing data sources that are either scarce, outdated, or siloed. Barriers include an over-dependence on personal connections for this access, the immaturity of available data platforms, the lack of data products from transactional systems, and the need for data protection and anonymization when exchanging or combining data with other entities, such as customers or partners. One respondent said: "I wish it was easier to access, normalize, validate and then extract value from [the] data refinery process." Another said: "I wish our systems would talk to each other." A third emphasized the need for "access [to] authoritative source data." Other views highlighted the importance of tools for labeling, validating, and standardizing datasets.

minute. Bottom line, data should be treated as a product, meaning that it is readily accessible and usable for current and future goals.[5] While DoD's internal data access issues are cultural and deep-rooted, requiring sustained commitment to resolve, this report offers aggressive remedies in an immediate effort to tackle data access challenges within the Department and across the defense industry.[6]

We therefore propose initial action around a new requirement in the fiscal year 2025 National Defense Authorization Act (NDAA) for all DoD vendor agreements to incorporate clear language on data rights and interoperability that manages data procured or generated under defense industrial contracts, and that facilitates, safeguards, and future-proofs DoD's access to this data. This will enable DoD to secure contractual rights to data acquired from commercial, subscription-based platforms, claim ownership of data generated through DoD-funded commercial technologies, and establish expansive rights for future data transformations and procurements. To foster favorable data marketplace conditions, this NDAA requirement should also direct the formation of a federated defense industrial data catalog for defense companies and the Department, a trusted community of interest for accessing this federated data catalog, and an oversight body for this new data marketplace. While DoD data access issues will not resolve overnight, enhanced collaboration with commercial vendors will propel DoD's antiquated approach to data access decades forward in the next 12 to 18 months.

Concurrently, to drive data access over the medium term, the DIB also recommends DoD-wide alignment to a set of ten "Chief Data and Artificial Intelligence Officer (CDAO) Principles" to standardize the Component CDAO talent lifecycle and provide an echelon-agnostic framework for utilizing data leaders within their organizations (the principles can be found on page 16). CDAOs are *the* key implementers of data best practices at the Component-level, but are scattered in their placement and utilization. These principles attempt to provide a framework for effectively integrating and empowering CDAOs across the defense enterprise.

Finally, the DIB recommends immediate implementation of a cohesive unit of specific recommendations in each of six core areas of the DoD data economy. If scaled properly, these solutions will catalyze improved data access and use for the warfighter.

- **LEADERSHIP: Empower the DoD CDAO to effectively lead.** Change is happening incrementally and not keeping pace with warfighting needs. While the DoD CDAO has seeded important efforts, such as the AI and Data Acceleration (ADA) initiative with the COCOMs, the organization is beset with challenges. The only way to achieve meaningful change in the DoD data economy is to ensure that the Pentagon's top data and AI executive is properly postured, consistently resourced, physically present, and has clear and measurable goals and objectives.
- **PEOPLE: Strengthen talent management to build data literacy at echelon.** Digitally native talent exists throughout DoD but faces barriers to effecting real change. Components should create environments in which civilian or military personnel can express their innovative talents without fear of reprisal. Services should develop promotional pathways for members willing to take risks that jeopardize their advancement,

[5] O'Regan, S. (2020, April 8). *Designing Data Products*. Medium. https://towardsdatascience.com/designing-data-products-b6b93edf3d23

[6] Many stakeholders referenced challenges with data acquisition due to outdated processes, manual workflows, or complex contracts, and desire a change to the culture mindset of people who are either resistant to new data technologies or over-reliant on old systems or habits.

and that reward unorthodox approaches to hard problems. Data literacy programs for new and existing personnel are crucial to improving data understanding and practices.

- **PROCESS: Incentivize data sharing through a cultural shift from systems risk.** DoD as an organization is neither structurally nor culturally equipped to effectively share data. Leadership should better articulate the balance between systems risk and data sharing and model data-centricity by embracing data analytics and dashboard-driven reporting. Components need to adopt a "responsibility-to-provide" data culture and improve data literacy among contracting officers.
- **TECHNOLOGY: Enable API-first architectures and technologies.** DoD should address its lack of data extensibility across environments by using Application Programming Interfaces (APIs) and large-scale AI tools to free data for the enterprise. API implementation and usage has become table-stakes for successful enterprises over the past decade – DoD needs to aggressively follow the same path. While DoD must maintain strict protocols to ensure the security of its systems, Components should balance data sharing with security requirements by streamlining enterprise applications in secure environments and building data visualization capabilities for administering data ownership and access at echelon. Data teams should also focus on improving the front-end user experience of these technologies.
- **INCENTIVES: Change profit opportunities by updating contract incentives.** Allow defense platform providers to profit from hosting third-party software, including data analytics and AI. Each service should create pathfinder programs to shift significant profit opportunities away from maintaining legacy software to continually improving software based on data feedback. This software should be routinely recompeted so that third party software providers have recurring options to deploy software for recurring revenue.
- **IMPLEMENTATION: Build service- and theater-level data capabilities at echelon.** All service CDAOs should report to their service secretaries and chiefs directly, not to their chief information officers. The haphazard hiring and placement of CDAOs across the MILDEPs and COCOMs, and their associated authorities and resourcing, hamstrings efforts to effectively implement data reforms for the warfighter. Ensuring all MILDEPs and COCOMs have a full-time, dedicated, and clearly defined CDAO billet that is effectively integrated at the secretary or commander's table is essential to scaling data best practices across the enterprise.

Current DoD leadership is committed to the data mission. It recognizes the central requirement of having capable talent in the cockpit, and the fundamental importance of access to data. The vast majority of the community understands the need for leveraging data better, faster, and cheaper, and we acknowledge and commend the data champions and stewards across the Department who we heard from – of which there were too many to meet with individually – who are working tirelessly to drive this critical mission forward.

These recommendations attempt to help accelerate some of the excellent work across DoD to incorporate modern data practices into routine operations. Data access, interoperability, and optimization are table-stakes for long-term warfighting effectiveness, and – to continue to be the best in the world – it is essential that the Department applies its finite resources and attention to the correct solutions.

Introduction

The Department of Defense (DoD) has grappled with building a functional data economy for decades. The 2003 *Net-Centric Data Strategy*[7] and 2007 *Information Sharing Strategy*[8] defined the foundations of a modern DoD data economy; the 2018 *Artificial Intelligence Strategy*[9] and 2020 *Data Strategy*[10] resurrected and framed the requirement for data-centricity in the context of renewed efforts to apply AI to decision-making; and the 2021 Deputy Secretary memo on "Creating Data Advantage"[11] and 2023 *Data, Analytics, and Artificial Intelligence Adoption Strategy*[12] reiterated the importance of applying data and AI products to the warfighting mission. While defense leaders increasingly recognize the challenges at hand, advances in data-centricity remain encumbered by policy, process, and cultural hurdles.

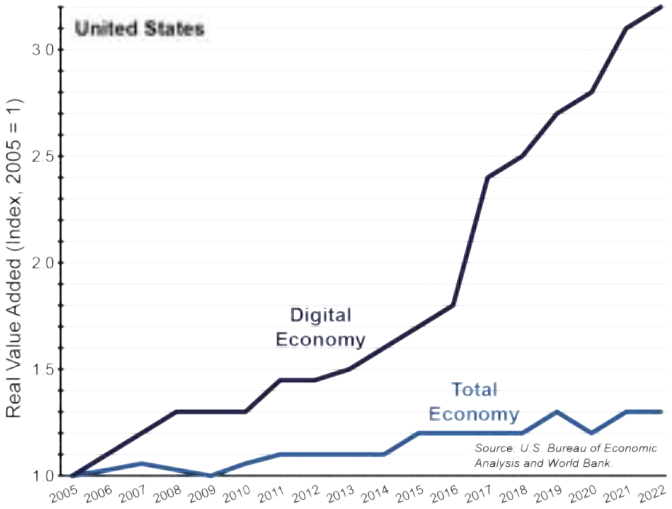

Figure 1. Digital Economy vs. Total Economy, Real Value Added[13]

Failure to scale adoption of modern data practices will hinder the Pentagon's efforts to counter pacing threats and defend the nation. DoD does not need more data strategies. Its senior leaders need to aggressively implement existing plans; promote and reward effective change where it is already happening; ruthlessly cut programs and personnel that are not driving the necessary reforms; and persistently hold Components accountable for their performance.

The Defense Innovation Board (DIB) set out to identify a set of recommendations in support of these important objectives. Over a 90-day sprint, we conferred with almost 100 data leaders across the Office of the Secretary of Defense (OSD), Military Services and Departments (MILDEPs), Combatant Commands (COCOMs), fourth estate defense agencies, and defense field activities. These included chief data and analytics officers, program executives, data architects and scientists, governance experts, and uniformed personnel at all echelons. We also heard from a wide range of innovation leaders from industry across the country, to include data and AI executives from large technology companies, the defense primes, non-traditional defense firms, and defense start-ups. We also collected insights from major universities and research institutions, including the Federally-funded Research and Development Centers. Finally, we closely engaged the DoD Chief Digital and Artificial Intelligence Officer (CDAO), the primary responsible party for advancing the

[7] Department of Defense, Chief Information Officer (2003, May 9), *DoD Net-Centric Data Strategy*
[8] Department of Defense, Chief Information Officer (2007, May 4), *Department of Defense Information Sharing Strategy*
[9] Department of Defense (2023, October 10), *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*
[10] Department of Defense (2020, September 30), *DoD Data Strategy*
[11] Department of Defense, Deputy Secretary of Defense (2021, May 5), *Creating Data Advantage*
[12] Department of Defense, Chief Digital and Artificial Intelligence Office (2023, November 2), *Data, Analytics, and Artificial Intelligence Adoption Strategy*

[13] This graph, demonstrating the exponential real-value growth of the U.S. digital economy relative to the U.S. national economy since 2005 (in 2005 chained dollars), affirms the mounting importance of data-centricity for economic prosperity – a fact mirrored in the national defense innovation ecosystem. Data is based on U.S. Bureau of Economic Analysis estimates of the size of the U.S. digital economy (2005-2016, adjusted 2009 dollars; 2017-2022, readjusted from 2017 to 2009 dollars) and World Bank estimates of U.S. gross domestic product (GDP).

Pentagon's adoption of best-in-class data, analytic, and AI capabilities.

The following pages encapsulate our conclusions regarding the current state of the DoD data economy, key recommendations for immediate consideration during the next defense budget cycle, and additional strategic proposals for optimizing the **leadership**, **people**, **process**, **technology**, **incentives**, and **implementation** aspects of this monumental effort.

Current State

Deputy Secretary of Defense Kathleen Hicks delivers remarks on innovation at the National Defense Industrial Association's Emerging Technologies for Defense conference Aug. 28, 2023. (Photo by: Department of Defense)

In December 2021, the Deputy Secretary established the DoD CDAO as the Department's data and AI lead.[14] With the Deputy Secretary's support, CDAO has enabled essential advances to data-centricity.[15] Today, the Deputy Secretary is beginning to evaluate her direct reports leveraging data from across the Department.[16] Within the MILDEPs, there are various data governance committees and standards-development projects underway to support adoption of data mesh and federated computational governance.[17] Across the COCOMs, there has been a similar emphasis on strengthening interoperability across services and theaters.[18] However, challenges abound.

[14] Department of Defense, Deputy Secretary of Defense (2021, December 8), *Establishment of the Chief Digital and Artificial Intelligence Officer*
[15] Department of Defense (2023, July 19), *Chief Digital & Artificial Intelligence Office Celebrates First Year* [Press release]. https://www.defense.gov/News/Releases/Release/Article/3464012/chief-digital-artificial-intelligence-office-celebrates-first-year/
[16] DIB interviews with anonymous DoD stakeholder (2023, September 20 and December 28).
[17] Department of the Army, United States Army Office of the Chief Information Officer (2022, October 13), *Army Data Plan*. https://api.army.mil/e2/c/downloads/2022/10/13/16061cab/army-data-plan-final.pdf; Vincent, B. (2023, March 22). Air and Space Forces lean into data-informed decision-making. DefenseScoop. https://defensescoop.com/2023/03/22/air-and-space-forces-lean-into-data-informed-decision-making/; Department of the Navy, Department of the Navy Chief Information Officer (2021, June 24), *Department of the Navy Actions to Data Advantage* https://www.doncio.navy.mil/ContentView.aspx?ID=14828
[18] USCENTCOM symposium spotlights the role of data on the battlefield. U.S. Central Command. (2021, February 23). https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/2512351/uscentcom-symposium-spotlights-the-role-of-data-on-the-battlefield/

DoD CDAO was established in late-2021 to replace or integrate the DoD Chief Data Officer, Joint Artificial Intelligence Center (JAIC), Defense Digital Service (DDS), Advancing Analytics (Advana), and Project Maven teams. Since becoming fully operational in June 2022, CDAO has undertaken a number of initiatives to accelerate the Pentagon's adoption of data, analytics, and AI. It has:

- Updated DoD strategy for data and AI to align with the 2022 *National Defense Strategy* (NDS).[19]
- Grew the Advana data analytics platform user base from 40,000 to 111,000 registered users.[20]
- Provided the Secretary and Deputy Secretary with the Pulse dashboard, an executive analytics capability in Advana, to enable data-driven performance evaluations at the highest level.[21]
- Continued developing data mesh policy and technology for the Combined Joint All-Domain Command and Control (CJADC2) data integration layer.[22]
- Embedded data teams within the OSD Principal Staff Assistants and unified Combatant Commands to support NDS implementation and leverage data and AI in operational environments.[23]
- Continued the Global Information Dominance Experiment (GIDE) series to test digital and AI systems in the field.[24]
- Funded AI battle labs to design and test new capabilities with warfighters in open and competitive environments.[25]
- Established Task Force Lima working-group discussions to assess methods and use-cases for employing generative AI tools, such as large language models.[26]
- Published a Responsible AI (RAI) Toolkit which identifies key efforts to operationalize DoD's *AI Ethical Principles*.[27]
- Promoted digital literacy through executive training programs for senior leaders and pilot programs to expand access to external data and AI coursework.[28]

On strategy and governance: existing guidance lacks detailed policy and technical instruction for appropriate standardization of the data economy. Despite various top-down and grassroots efforts at modeling data-centricity, the Department-wide plan for selecting and scaling adoption of specific efforts remains unclear beyond the broad principles articulated in prior strategies.[29] While these documents envision an end-state for the DoD data economy, they do not identify specific approaches to data access, analytics, and talent development. DoD also needs to accelerate and provide a more definitive plan for adoption of cutting-edge capabilities such as generative and multimodal AI. The answer should not be a data and AI policy that webs its way across the entire data economy; a single standard neither fits the Department's needs nor enables use of commercial data mesh environments. That said,

[19] Department of Defense (2024, January 9), DOD Increases AI Capacity Through Strategy, Alignment [Press release]. https://www.defense.gov/News/News-Stories/Article/Article/3639685/dod-increases-ai-capacity-through-strategy-alignment/
[20] According to data provided by the CDAO Advana team (2024, January 4).
[21] Demarest, C. & Gould, J. (2023, February 3). *Pentagon takes own 'Pulse' with internal data dashboard*. Defense News. https://www.defensenews.com/pentagon/2023/02/03/pentagon-takes-own-pulse-with-internal-data-dashboard/
[22] Harper, J. (2023, October 26). Pentagon's CDAO queries industry about commercial data-mesh capabilities. Defense Scoop. https://defensescoop.com/2023/10/26/pentagons-cdao-queries-industry-about-commercial-data-mesh-capabilities/
[23] Statement of Dr. Craig Martell, Chief Digital and Artificial Intelligence Officer Regarding How Federal Agencies are Harnessing Artificial Intelligence, House Oversight Committee on Cybersecurity, Information Technology, and Government Innovation. (2023). https://oversight.house.gov/wp-content/uploads/2023/09/DoD-Statement-House-Oversight-Final.pdf
[24] Bennet, J. (2023, December 15). *DOD CDAO Wraps Up 8th Global Information Dominance Experiment for CJADC2*. Executive Gov. https://executivegov.com/2023/12/dod-cdao-wraps-up-8th-global-information-dominance-experiment-for-cjadc2/
[25] Department of Defense (2023, September 27). *DOD to Establish AI Battle Labs in EUCOM, INDOPACOM* [Press release]. https://www.defense.gov/News/Releases/Release/Article/3540283/dod-to-establish-ai-battle-labs-in-eucom-indopacom/
[26] Vincent, B. (2023, November 6). *Inside Task Force Lima's exploration of 180-plus generative AI use cases for DOD*. Defense Scoop. https://defensescoop.com/2023/11/06/inside-task-force-limas-exploration-of-180-plus-generative-ai-use-cases-for-dod/
[27] Johnson, M. K., Hanna, Michael, M., Clemens-Sewall, M. V., & Staheli, D. P. (2023). Responsible AI Toolkit (RAI Toolkit 1.0), Responsible AI, US Department of Defense, Arlington, VA, [Online], https://rai.tradewindai.com
[28] Schehl, M. (2022, September 2). *NPS, Partners Develop Executive Course on AI/ML Foundations for Senior Leaders* [Press release]. Naval Postgraduate School. https://nps.edu/-/nps-partners-develop-executive-course-on-ai-ml-foundations-for-senior-leaders; Department of Defense (2023, November 16). *Chief Digital and Artificial Intelligence Office Launches Access to Digital On-Demand Learning Platform* [Press release]. https://www.defense.gov/News/Releases/Release/Article/3590669/chief-digital-and-artificial-intelligence-office-launches-access-to-digital-on/
[29] DIB engagement with anonymous DoD stakeholders (2023, October 27).

the DoD data economy needs a single, full-time, mission-focused leader with well-articulated authorities and a clearly defined chain of command to provide a unified approach to this organizational change. This leader, whether at the CDAO or Component-level, should possess broad technical knowledge, a nuanced perspective on systems risk versus data access, demonstrated leadership in and a strong grasp of both private- and public-sector dynamics, and the ability to build consensus within large entrenched bureaucracies.

On technology and architecture: there is an over-prioritization of large, bulky, platform-centric solutions with a selective focus on exquisite data and software requirements. While the Deputy Secretary's 2021 "data decrees" have accelerated the process of centralizing data management, too many systems at the tactical edge still lack Application Programming Interfaces (APIs) and other domain-driven approaches for freeing data to the enterprise.[30] Slow, uneven adoption of federated computational governance exacerbates these difficulties as a plethora of data models and taxonomies which are poorly tied to joint system requirements attempt to fill the void.[31] DoD needs an integrated capability framework that keeps pace with the data innovation occurring at the edges. To ensure greater uniformity of data and software requirements, this framework should be nested with the Joint Warfighting Concept and other joint documents that provide an authoritative menu of approved joint mission threads and required system functions.[32] The Deputy Secretary's Pulse initiative, using data analytics

The 50th Expeditionary Signal Battalion conducted a combined Large Scale Combat Operations (LCSO) communications exercise on Fort Liberty, North Carolina as part of recurring Scarlet Dragon Oasis AI-enabled live-fire target identification exercises. (Photo by Capt. Eric Messmer, U.S. Army)

to evaluate implementation of DoD's *Strategic Management Plan*[33] (SMP) guiding four-year implementation of the NDS, has the clearest potential for ensuring that new data mesh requirements for the CJADC2 data integration layer are properly tracked and resourced at the highest level.

[30] DIB engagements with anonymous DoD stakeholders (2023, October 27 and December 8).

[31] The Army's Unified Data Reference Architecture (UDRA) is one effort to move closer toward unifying data mesh and leveraging emerging data fabric capabilities. Similarly, the Air Force has made progress in defining plans for its Advanced Battlefield Management System (ABMS) in support of CJADC2. The Navy is also updating plans for its data architecture. Perez, L. (2023, October 12). *Army Seeks Insight on Building Unified Data Architecture*. MeriTalk. https://www.meritalk.com/articles/army-seeks-insight-on-building-unified-data-architecture/; Gill, J. (2023, August 8). *Air Force developing new architecture for JADC2 'kill chains,' wants faster ABMS development*. Breaking Defense. https://breakingdefense.com/2023/08/air-force-developing-new-architecture-for-jadc2-kill-chains-wants-faster-abms-development/; Vincent, B. (2023, October 16). *Navy preps new strategic 'blueprint' for its ever-changing information architecture*. Defense Scoop. https://defensescoop.com/2023/10/16/navy-preps-new-strategic-blueprint-for-its-ever-changing-information-architecture/

[32] The Universal Joint Task List provides the authoritative menu of approved joint tasks, and the Joint Common System Function List defines the necessary system functions. DIB interviews with anonymous DoD stakeholders (2023, July 19 and August 25).

[33] Department of Defense, Deputy Secretary of Defense (2022, October 28), *DoD Strategic Management Plan*

Lastly, on people and partnerships: organizational leaders lack a basic understanding of data, innovators often feel disempowered, and capable personnel are not being properly utilized. While DoD has an abundance of digitally native talent, innovative potential, much less data expertise, is not judged favorably against other traditional markers for promotion.[34] There is little engagement between military personnel and industry, and what engagement that occurs often begins too late in a service member's career to provide meaningful value to the technology research, development, and acquisition process.[35] Too often, data specialists and other digital natives feel constrained by an institutional bias toward systems security and data hoarding, and lack adequate top cover and resources for developing new programs that effectively share data and deliver data-driven effects to the warfighter.[36] Likewise, access to modern software tools and environments necessary for this experimentative work remains restricted, and when innovation does occur, there are limited means for sustaining further digital transformation.[37]

[34] Research from the Center for Security and Emerging Technology (CSET) and MITRE Corporation found that although DoD is a top employer of technical talent in the United States, the real challenge is that many specialists are hidden and underutilized. Gehlhaus, D., Hodge, R., Koslosky, L., Goode, K., & Rotner, J. (September 2021). *The DOD"s Hidden Artificial Intelligence Workforce*. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/the-dods-hidden-artificial-intelligence-workforce/

[35] DIB engagement with anonymous industry stakeholders (2023, December 1).

[36] Gehlhaus, D. (2022, February 16). *To get better at AI, get better at finding Ai talent*. Defense One. https://www.defenseone.com/ideas/2022/02/get-better-ai-get-better-finding-ai-talent/362059/

[37] DIB interview with anonymous DoD stakeholder (2023, November 28).

Recommendations

Data is a strategic asset and should be treated as a product, yet prevailing DoD approaches to data access remain severely outdated. The Department operates numerous legacy systems that are often incompatible with one another, slow at data processing, and challenged with difficulties in data storage and retrieval. This has led to the stunning realization that, in certain situations, the United States Postal Service remains the fastest and most reliable network for big data transfers, and that moving data onto hard drives or even DVDs is still the quickest way for combining data from different networks.[38] While security is a paramount consideration, existing security classification guidance is broken, either misaligned with DoD guidance, nonexistent, or riddled with errors, contributing to further delays in decision-making.[39] Different branches and units have their own systems and protocols, making decentralization a contributing factor to inconsistencies and gaps in the data. Finally, cultural and organizational barriers to data sharing, combined with a shortage of personnel with training in modern data handling and analytics, hinders effective strategic planning and joint operations.

> **Data Access: Frustrated Users' Perspectives**
>
> "We have an innovation cell that acts as a dragnet for ideas at the tactical level. If we are talking about data-related projects, honestly, many actors put the 'no' in innovation – often it's not the person, but the rules the person follows. I can't tell you how many Airmen have come to me with app ideas, sometimes even having coded them themselves. Then 'cyber' does the equivalent of "What if the Russians get into the database?" at which point we say, "Yep, you're right, we'll go back to pen and paper. Sorry to bother you." So, because of the way cyber goes about treating anything new, we focus mostly on non-data-related innovations. In fact, I probably shouldn't say this but having been through (mostly) unsuccessful experiences, I don't encourage working on anything computer related." –*Anonymous DoD warfighter*
>
> "As a naval architect … much of the data I interact with is stovepiped and/or not digitized. For example, the vast majority of towing tank data from before the 1990s exists as paper reports, printed graphs, etc. that are held in inaccessible repositories. I'm very concerned that, due to poor data sharing, we are losing valuable knowledge and lessons learned. Looking ahead at the future of warship design, I'm concerned that we are still following our old practices of data stovepiping and inconsistent data formatting." –*Anonymous DoD civilian*
>
> "Having worked [in data leadership roles across Big Tech] while concurrently supporting DoD from my reserve role as an AI product manager, I see that the Department will continue to be challenged in training and acquiring data talent due to the high friction points of being able to use the data easily … internal inertia and the inherent way talent is managed today encourages a siloed and risk-averse approach versus an innovative and collaborative partnership." –*Anonymous industry data leader*
>
> "DoD is not prepared to staff data stewards, curators, and architects at the level that will be needed if data is to become a trusted warfighting asset. Appropriate trust is needed if shared data is to be useful. The U.S. fights within a coalition and appropriate guardrails must be put in place if data is to be safely and securely shared at speed and at scale with our allies." –*Anonymous military futures strategist*

While a DoD-wide data access standard would not afford the flexibility for Components to meet their specific access requirements, this study's overarching recommendation is that in order to build a robust data economy, DoD must first address its lack of seamless data extensibility and interoperability through a unified, scalable data access approach. As DoD's internal data access issues require sustained commitment to resolve, this report recommends an initial focus over the next 12 to 18 months on improving data access collaboration with commercial vendors.

[38] DIB interview with anonymous DoD stakeholder (2023, November 28).
[39] Examining the Costs of Overclassification on Transparency and Security: Hearing before the Committee on Oversight and Accountability, 114th Congress. (2016). https://oversight.house.gov/hearing/examining-costs-overclassification-transparency-security/

Effecting the necessary change over this period requires a fundamental shift in DoD's approach to data access with industry partners that should be enshrined in legislative action through the forthcoming National Defense Authorization Act (NDAA).

NDAA Data Access Requirement

The current state of data access within DoD vendor agreements is fragmented and inconsistent, and DoD does not have sufficient data rights such that it can aggregate and ensemble data from various platforms and services for future data transformations.[40] In particular, DoD faces notable challenges in accessing and managing data originating from systems it subscribes to or builds in collaboration with industry. Beyond its specific contractual obligations and limitations, DoD lacks access to a catalog of defense industrial data for providing a comprehensive picture of government-funded defense technology research and development.[41]

Secure Contractual Rights

Secure contractual rights to operational and business analytic data obtained from commercial platforms that DoD subscribes to.

R&D Data Ownership

Claim ownership of data generated through commercial technologies developed using DoD research, development, test, and evaluation funding.

Future Data Ownership

Establish expansive access for future data transformations and data ensembles.

Exhibit A. Key Pillars of DoD Data Access: Prevailing DoD data access approaches are outdated, inhibiting effective interoperability and utilization of data across various platforms to enable Combined Joint All-Domain Command and Control (CJADC2).

Without a central node at the Pentagon with streamlined access to aggregated defense industrial data, DoD program managers will continue to struggle at identifying connections and entry points for potential industry collaboration, leading to further inefficiencies and missed opportunities for harnessing new solutions at the tactical edge. Key stakeholders within industry, both defense primes and newer players, have also emphasized the value of a data catalog for helping them monetize their existing program data to identify new opportunities for more rapid collaboration.[42]

In keeping with the urgency of this challenge, the DIB recommends for DoD and Congress to work through the next NDAA to incorporate clear language on DoD data rights for managing data procured or generated under federal defense contracts. Additionally, DoD and Congress should establish a new marketplace for defense industrial data that sets market conditions and incentives for data access and sharing within the broader defense innovation ecosystem. In particular, this NDAA requirement would:

[40] DIB engagement with anonymous industry stakeholders (2024, January 5)
[41] DIB engagement with anonymous industry stakeholder (2024, January 5)
[42] DIB engagement with anonymous industry stakeholders (2023, December 1 and 2024, January 5)

1. *Secure contractual data access for DoD.*
    - Mandate DoD rights to data obtained from commercial, subscription-based platforms.
    - Claim ownership of data generated through DoD-funded commercial technologies.
    - Establish expansive rights for future data transformations and data ensembles.
2. *Set data sharing incentives for industry.*
    - Implement sophisticated data monetization methods (e.g. royalty-based licensing agreements, performance-based contracts, discount-pricing models) to incentivize industry data sharing.
    - Encourage trusted industry partners to avail their data to foster research collaboration.

To set conditions for this data marketplace, this NDAA proposal should include:

3. *A federated data catalog for defense technology: a multi-vendor data catalog integrating data sources from across the defense industrial base enterprise.*
    - This catalog will serve as a central repository for defense technology industrial data, enhancing accessibility and interoperability between DoD industry partners.
4. *A trusted community of interest for accessing this federated data catalog: a central community comprising vendors, warfighters, and acquisition program executives.*
    - This community will facilitate collaboration on requirements, concepts of operation, and design processes, ensuring early exposure of end-users to the development phases.
5. *An independent oversight body for this new data catalog and community of interest.*
    - This body will ensure compliance with data access requirements, maintain strict controls over sensitive proprietary data, and foster continuous improvement in data management practices.

Chief Data and Artificial Intelligence Officer (CDAO) Principles

Concurrently, to drive data access over the medium term, the DIB recommends adoption of the following set of "CDAO Principles" to provide DoD organizations with an echelon-agnostic framework for how data leaders across Components are selected, integrated, utilized, and managed.

1. **Recognize Data as a Product.** DoD organizations and their CDAOs will recognize data as a product in order to effectively translate the commercial mindset of monetizing data to DoD's mindset of leveraging data to achieve rapid battlefield effects.
2. **Prioritize Diverse Expertise.** Organizations will select CDAO candidates who combine industry with public sector experience to ensure broad familiarity with DoD culture and norms, mastery of technical competencies, strategic acumen, and other essential leadership qualities.
3. **Define Responsibilities Early.** Organizations and their CDAOs will establish a clear understanding of the CDAO function's major duties, responsibilities, and supervisory relationships.
4. **Assess Data Readiness.** CDAOs will conduct a technical posture assessment of their organization's data readiness to improve understanding of organizational needs and prepare an action plan.

5. **Develop and Execute Strategy.** CDAOs will craft a strategic roadmap tailored to their organization's data readiness that progresses data maturity and governance across key dimensions of the data economy including process, people, and technology.
6. **Align Data and Technology.** CDAOs will be operationally aligned with, but not report to, their organization's Chief Information Officer (CIO) or Chief Technology Officer (CTO).
7. **Implement an API-First Strategy.** CDAOs will integrate APIs into all technology projects in their organizations to ensure all systems are inherently designed for data access and interoperability.
8. **Connect Data to Cutting-Edge Services.** CDAOs will leverage artificial intelligence (AI) and machine learning (ML) capabilities to enhance data analytics services in their organizations, while adhering to strict ethical and security standards.
9. **Foster the Founder's Mindset.** CDAOs will model and promote a culture of experimentation, curiosity, and entrepreneurship among all personnel in their organizations.
10. **Model Data-Centricity in Action.** CDAOs will ensure that their commanders and deputies lead by example through embracing data-driven methods in all aspects of routine operations.

Data requirements and uses are often unique to their organizations, and what works for one team will often not work for another. While there is not a single approach that can be formulaically applied across DoD's vast data economy to achieve the same effects, this framework of principles can be used as a guide for DoD entities to standardize the Component CDAO talent lifecycle – from recruitment to execution – to bring in uniquely tailored data leaders to address their unique data challenges.

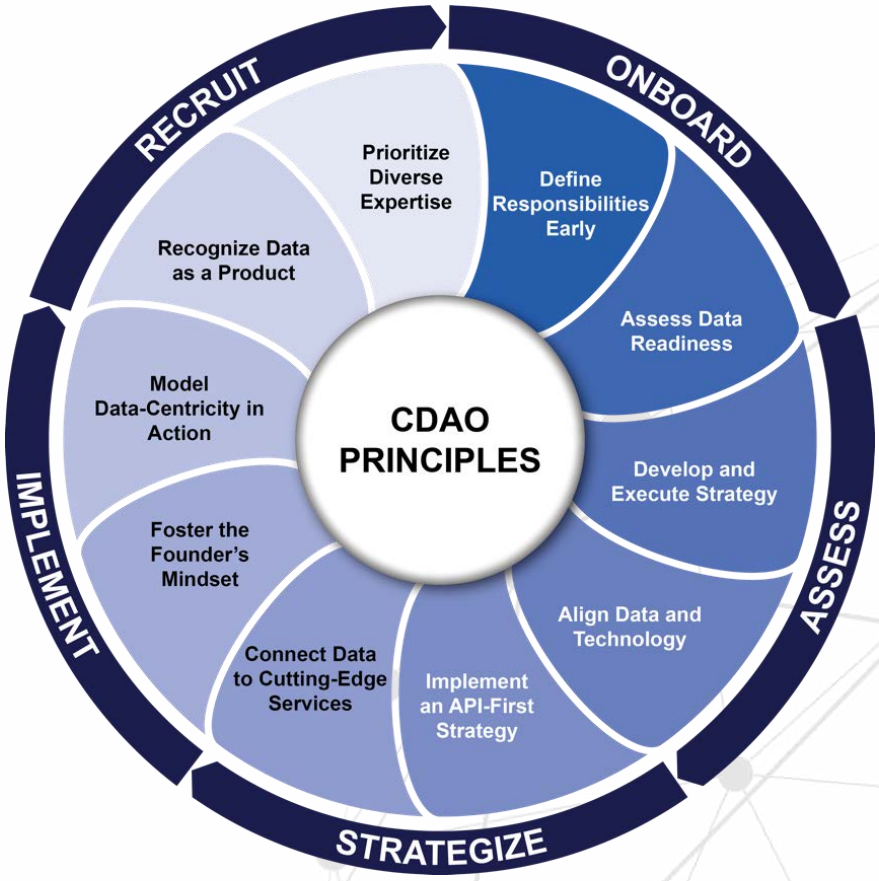

Exhibit B. CDAO Principles

Additional Strategic Proposals

Beyond working with Congress and industry on data access, we recommend that DoD adopt the following set of proposals across six core areas of **leadership**, **people**, **process**, **technology**, **incentives**, and **implementation**. Adopted as a cohesive unit, these actions would ensure that DoD data leaders are properly elevated and resourced, erode poor data-sharing practices, expand the community of data stewards, modernize data architecture, update data rights contracts, and address concomitant obstacles to implementation.

LEADERSHIP: Empower the DoD CDAO to effectively lead.

Throughout our discussions with data users at the operational edge, we repeatedly heard that change is happening too incrementally to keep pace with warfighting needs. It took over two years after the 2021 "data decrees" for the Deputy Secretary to commence routine data-driven evaluations of the OSD Principal Staff Assistants using the Pulse executive analytics dashboard.[43] Importantly, we heard that these routine updates to the Deputy Secretary have provided her with constructive and revealing customer feedback than what CDAO is demonstrating on key data initiatives that are lagging.[44] Indeed, while CDAO has helped seed important efforts, such as the AI and Data Acceleration (ADA) initiative with the COCOMs, the organization has been beset by challenges. The current CDAO is based on the West Coast, similar to the director of the Defense Innovation Unit (DIU). While this arrangement potentially works well for DIU, which provides the connective tissue between DoD and Big Tech, CDAO's role as *the* data and AI leader for the Department makes its presence at headquarters imperative. To effectuate real change, there is no substitute for persistent, personal involvement from the Pentagon's top executives.[45]

To further strengthen CDAO's data stewardship, CDAO's *statutory* data roles and responsibilities as the DoD CDO also require additional clarification. The Deputy Secretary's original memo establishing CDAO instructed the DoD CDO to be "operationally aligned" to the new organization while still reporting to the DoD Chief Information Officer (CIO) pursuant to Section 903(b)(3) of the FY 2020 NDAA.[46] The CIO reporting language was struck from the FY23 NDAA, and today, the CDAO and DoD CDO entities are functionally identical and report directly to the Deputy Secretary. Critically, however, existing guidance still makes it unclear what CDAO's exact authorities are as the DoD CDO beyond – in accordance with the FY20 NDAA – guaranteeing it "access to all DoD data."[47] Furthermore, CDAO is often confused as a primarily AI-focused entity, not *the* manager of data across the Department. This creates confusion as to CDAO's remit, beyond setting overall data strategy and policy, for enforcing necessary changes to the ecosystem.

We therefore recommend the following enhancements to CDAO's existing posture:

1. The CDAO should be headquartered at the Pentagon and key supporting personnel should occupy consolidated floor space in the National Capital Region to improve the organization's integration.
2. In lieu of a dedicated senior leader on the West Coast, the CDAO may establish a national liaison network aligned to DIU's

[43] DIB interview with anonymous DoD stakeholder (2024, January 2).
[44] For example, we heard dissatisfaction with the pace of development of classified data and analytics environments within Advana. Users complained that most CDAO data products are still at the NIPR (Unclassified) level, with limited access at the SIPR (Secret) much less the JWICS (Top Secret) levels. According to CDAO, there are currently about 475 business systems at the NIPR level and 50 at the SIPR level. Stakeholders noted that Advana JWICS environments are either nonexistent, not widely known, or difficult and time-consuming to access.

[45] Department of Defense, Defense Innovation Board (2023, July 17), *An Innovation Strategy for the Decisive Decade*
[46] Department of Defense, Deputy Secretary of Defense (2022, February 1), *Initial Operating Capability of the Chief Digital and Artificial Intelligence Officer*
[47] S.1790 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2020. (2019, December 20). https://www.congress.gov/bill/116th-congress/senate-bill/1790

footprint – e.g. in Silicon Valley, Boston, Austin, and Chicago – to strengthen this broader engagement.

3. To oversee this expansion, the CDAO should have not one but two principal deputies functioning as the organization's chief operating officer and chief technology officer. Target individuals for these key roles (and others) that demonstrate a combination of deep technical competence in data and AI along with leadership experience across both public and private organizations.
4. The Deputy Secretary should issue a memo clarifying CDAO's data roles and responsibilities beyond "access to data."
5. The Deputy Security should convene with CDAO a recurring Deputy's Management Action Group focused on data to begin routine evaluations of data leaders across the MILDEPs and COCOMs.
6. Once these actions are taken, the CDAO may be given oversight of a central data funding line to dispense resources to data activities across the Components, and report back monthly on fund allocations and mission progress.
7. Finally, the CDAO's ADA teams should have clearly defined responsibilities within their respective COCOMs. Each ADA team should sign a memorandum of agreement aligned to their COCOM's specific data needs to support effective utilization of this important initiative.

PEOPLE: Strengthen talent management to build data literacy at echelon.

We challenge the prevailing notion that DoD cannot compete with industry for the best and brightest data talent. While recruitment offices face significant hurdles, be it salary or security clearance adjudication, there is an abundance of untapped talent within the ecosystem.[48] Current warfighters and DoD civilians are brimming with ideas and care deeply about the data mission, and industry's ranks are replete with veterans, reservists, and former public servants.[49] It is up to DoD's data and AI functional community managers to tap into this wellspring and to provide a more structured whole-of-ecosystem approach to strengthening data literacy across echelons.

While there are various independently organized opportunities for warfighters to acquire data-related skills – e.g. at Army Software Factory[50], AFWERX[51], and West Point's "Data Literacy 101" seminar[52] – there is often no berth for those skills. Abilities atrophy, knowledge becomes out-of-date, personnel are knocked off the promotion path, and without official guidance, this multiplying network of upskilling efforts will remain disconnected and underfunded.

DoD civilians have more natural pathways for career advancement, but still face barriers to effecting change. Confined by senior leadership uncomfortable with the pace of technological evolution, they often lack the necessary avenues for experimenting and (responsibly) breaking things.[53] In particular, Highly Qualified Expert (HQE) personnel are relied on for their

[48] Weisner, M. (2023, October 26). DOD hindering recruitment of tech-savvy workers, warfighters: Report. Federal Times. https://www.federaltimes.com/management/career/2023/10/26/pentagon-practices-harm-recruitment-of-tech-savvy-workers-warfighters/

[49] DIB engagement with anonymous industry stakeholders (2023, December 1).

[50] Errico, V. (2023, June 21). *Software Factory Direct: Program Brings Cutting-Edge Technology to Soldiers*. Association of the United States Army. https://www.ausa.org/articles/software-factory-direct-program-brings-cutting-edge-technology-soldiers

[51] Fetter, J. (2019, December 27). *Project Nexus: Empowering the Air Force's Digital Talent*. Joint Base San Antonio News. https://www.jbsa.mil/News/News/Article/2019258/project-nexus-empowering-the-air-forces-digital-talent/

[52] Dower-Rogers, M. (2023, August 2). *West Point Center for Data Analysis and Statistics Hosts Data Literacy Training Event for Army Leaders*. United States Military Academy West Point. https://www.westpoint.edu/news/academic-news/west-point-center-data-analysis-and-statistics-hosts-data-literacy-training

[53] DIB interviews with anonymous DoD stakeholders (2023, November 28).

technical expertise, but usually lack proper authorities and resources.[54]

Even as DoD continues to allocate more resources and billets for data professionals when appropriate, it is equally imperative to raise salaries in order to attract the most qualified candidates. A recurring theme from our discussions was the challenge not solely in filling vacant data billets, but in filling them with adequately experienced and skilled candidates. While the broader aspects of the talent hiring issue fall beyond the scope of this report, it is essential for us to highlight salary as a crucial factor in the recruitment and retainment of top-tier talent and a key driver of long-term workforce efficiency.

Ultimately, however, great talent is always attracted to great missions. Securing the future of democracy and the safety of America's and the world's citizens is a great mission. We need to galvanize, break glass, and ensure we execute effectively and efficiently. To better unleash the workforce's potential, the DIB recommends the following actions:

1. Introduce a "Data Officer" Military Occupational Specialty (MOS) to provide a clear pathway for data professionals to progress their military careers and showcase their contributions. In doing so, the services will retain more talent which is currently leaving for industry, and better integrate data readiness at the operator level.[55] Data should not rest solely at the level of business analytics and, rather, is an essential component of the warfighting function (e.g. Project Fox live-streaming F-35 Lightning II data to a connected computer tablet).[56] Failure to provide viable career pathways for individuals able to make this connection will hinder DoD's digital transformation.
2. Create environments in which personnel can express their innovative talents without fear of reprisal for security infractions. Components should model examples of successful innovation pipelines (e.g. AFWERX Spark Cells[57], SOCOM Ignite[58]) as well as invest further in collaborative experiences (e.g. AFWERX Challenge[59], BRAVO hackathons/AI battle labs at EUCOM and INDOPACOM[60]). They should also provide workplace-accessible environments for pushing the limits of innovation (e.g. air-gapped "channels" to experiment with untrusted tools such as new generative AI applications).[61]
3. Form a CDAO "head-hunter" support function to assist Components with CDAO recruitment and coaching. Currently, Components do not have a sufficient understanding of the candidate attributes required to fill their CDAO billets. This function could incorporate a panel from various DoD expert organizations in technology, innovation, and management, to include CDAO, DIU, the recently established Defense Management Institute, and individual special government employee (SGE) consultants. While this entity should not take over hiring of CDAOs on behalf of Components, it can provide objective, impartial advice to improve matching of candidates to organizations.

[54] DIB interview with anonymous DoD stakeholder (2023, December 13).
[55] DIB engagement with anonymous industry stakeholders (2023, December 1).
[56] Sutter, J. (2021, April 19). *Reserve airman makes history with innovative project Fox/F-35 development*. United States Air Force [Press release]. https://www.af.mil/News/Article-Display/Article/2577421/reserve-airman-makes-history-with-innovative-project-foxf-35-development/
[57] Spark cells. AFWERX. (2023, December 1). https://afwerx.com/divisions/spark/spark-cells/
[58] FY24 SOCOM Ignite Challenges | SOCOM Ignite. (n.d.). https://ignite.ll.mit.edu/ignite/operator-challenges-fy24
[59] Shapiro, B. (2024, January 5). AFWERX Challenge serves as catalyst for future technology advancements. United States Air Force. https://www.arnold.af.mil/News/Article-Display/Article/3636750/afwerx-challenge-serves-as-catalyst-for-future-technology-advancements/
[60] Harper, J. (2023, December 7). Hackathon at Indo-Pacific Command's new AI battle lab open to all US citizens. Defense Scoop. https://defensescoop.com/2023/12/07/hackathon-at-indo-pacific-commands-new-ai-battle-lab-open-to-all-us-citizens/
[61] DIB interviews with anonymous DoD stakeholders (2023, November 28 and December 13).

The SOCOM Ignite Program brings together young service members, university faculty and students, and technologists to develop new capabilities for Special Operations Command. Here, Air Force and Army cadets learn about robotic systems at the Lincoln Laboratory's autonomous systems development facility on Hanscom Air Force Base. (Photo by: Glen Cooper, MIT Lincoln Laboratory)

4. Empower HQEs with greater employment protections and options for extended terms. Presently, HQEs are afforded weak at-will employment protections in addition to term-limits that are difficult to renew.[62] Combined with a lack of management and enforcement authorities, these individuals are often limited in impact. Getting top talent in the door is essential, but proper empowerment and support is required for their success.
5. Issue guidance to allow the use on DoD systems of basic developer tools, such as Python, Github, Bootstrap, Chrome DevTools, Azure, and AWS Cloud9. We heard complaints that, currently, data engineers lack access to essential developer environments, and interested professionals who register to take classes on programming run into firewalls around basic tools for completing their coursework.[63]
6. Develop a pilot Defense Data Management Training Module intended for all DoD civilians, military, and contractors. Developing a concrete understanding of data should be a core mission of workforce training. Existing training modules only focus on data protection, without providing a broader sense of where and how personnel fit into the data production process.[64] When DoD employees onboard, they should develop a foundational awareness of how they contribute to the data value chain.

PROCESS: Incentivize data sharing through a cultural shift from systems risk.

Below the senior leader level, two key behaviors are hindering data-centric modernization efforts. Foremost is a common failure to treat data as a product and to truly grasp the importance of availing data for future uses hitherto unknown. While program managers and domain experts will aggregate information to recognize trends and identify optimizations, their narrow focus on systems security will often contribute to further data hoarding.[65]

Second is the Department's bias toward systems protection which further impedes efficient data sharing.[66] Data professionals and other personnel spend significant time up- and down-domaining data, shifting data between platforms, and worrying about the constraints surrounding data rather than productizing this information for the warfighter.[67] While cyber protection, systems security, and proper handling of PII and other sensitive information are essential, DoD should better balance systems security and data use.

In order to strengthen data sharing in accordance with reasonable access controls, the DIB recommends the following actions:

[62] DIB interviews with anonymous DoD stakeholders (2023, November 28)
[63] One stakeholder noted: "Our talent is unable to take a Coursera class and download necessary Python packages to complete the course. We have classes we pay for through Digital University, and then we literally run IT machines that prevent them from even trying or employing what they learn."
[64] DIB interview with anonymous DoD stakeholder (2023, November 9)
[65] DIB interview with anonymous DoD stakeholder (2023, November 7)
[66] Vandiver, J. (2023, March 29). Classifying information for no good reason is hurting military effectiveness, report warns. Stars and Stripes. https://www.stripes.com/theaters/us/2023-03-29/military-classified-documents-9639844.html
[67] DIB interview with anonymous DoD stakeholder (2023, November 28)

1. Update Deputy Secretary guidance on data access to direct the Department to transition from a "need-to-know" approach to data security to a "responsibility-to-provide" framework more aligned with the modern warfighter's requirement for data to be freed from siloed systems.
2. Establish within each Service a "super program executive office (PEO)"[68] (e.g. a PEO Digital) to prioritize the transfer of modern software development experience to a portfolio of legacy products.[69]
3. Decouple data management from cybersecurity and systems security to balance data access and protection. CDAOs should define or mandate system and solution requirements for every material acquisition and some if not all non-material acquisitions. Start with simple things like common data ownership and use-language in contracts, then branch out into standardizing information protection guides rather than security classification guides.[70]
4. Encourage the development of tools to streamline the data production and management lifecycle (e.g. Project Battering Ram to automate classification determinations).[71]
5. Mandate data literacy training for contract officers and acquisition specialists. Procurement officers should financially incentivize good data practices from industry partners, ensure that data is treated as a service and not a one-time obligation, and better articulate the overall value of data.[72]
6. Leadership implementation of a dashboard- and data-driven presentation culture. All senior leaders (commanders, deputies, chiefs of staff, etc.) should task their reports to use data analytics tools when briefing, recognizing that any presentation to leadership within PowerPoint is a point of data failure.[73]
7. Authorize public reporting on successes and failures. Both by unit and community, organizations need a report card that has all eyes on it and leaders that define what success looks like.[74]

TECHNOLOGY: Enable API-first architectures and technologies.

DoD needs to improve data centralization and integration within a federated, domain-driven architecture. Many stakeholders expressed preference for data to be centrally accessible from a single location and to be able to join and integrate data from various vendor solutions and even with foreign partners. Many mentioned the need for data tagging and filtering based on utility and relevance, with suggested solutions ranging from creating a DoD Joint Data Library and digitizing historical data to leveraging distributed ledger technologies to unlock data silos. Most stakeholders also agreed that DoD is starved for relevant data and analytics capabilities. There was broad consensus that faster, more efficient, and insightful data processing and analysis tools which, for example, can automate and streamline data acquisition, are necessary to ensure that relevant operational data is provided to the

[68] The Atlantic Council Commission on Defense Innovation Adoption's interim report recommended a "capability portfolio model … [including] a command-and-control PEO that invests in a software factory and enterprise services as a common infrastructure." Lofgren, E., McNamara, W. M., & Modigliani, P. (2023, April 12). Commission on Defense Innovation Adoption Interim Report. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption-interim-report/

[69] A similar set of recommendations regarding legacy products were also issued in an August 2021 report by the Defense Digital Service assessing Transportation Command, Air Mobility Command's digital operations. DIB interview with anonymous DoD stakeholder (2023, December 13).

[70] DIB interview with anonymous DoD stakeholder (2023, November 7).

[71] DIB interview with anonymous DoD stakeholder (2023, November 28).

[72] DIB engagement with anonymous industry stakeholders (2023, December 1).

[73] DIB interview with anonymous DoD stakeholder (2023, December 13).

[74] Ibid.

warfighter in trusted, accessible, and empowering user environments.[75]

Bridging the gap between current operations and systems of record is imperative. At present, data requirements are not sufficiently tied to system requirements.[76] For example, stakeholders mentioned problems with basic back-office functions, such as maintaining an accurate picture of personnel and billets.[77] Current systems of record, such as DCPDS, AOS, and IPPS-A, are not easily accessible in one location, and do not track personnel and associated positions at the level of granularity required.[78] There also needs to be better traceability of warfighting needs and gaps to the responsible services. Too often technology is not built and delivered to the user as an architecture, thus contributing to data hoarding. Service members need applications with a human (i.e. warfighter)-centric design that does not require users to be experts in the data, but rather adapts natively to their needs.[79] Ground-up initiatives that provide strong ease of use, demonstrated core functionality, and a just-works user experience are essential for building a data exchange mindset and continuous interoperability.[80]

With regards to Advana we heard concern that large, centralized platforms often create more silos and blockers than they remove. Additionally, Advana JWICS remains a serious functional gap.[81] CDAO has focused on building NIPR and SIPR capabilities (where the majority of DoD employees reside), but has yet to scale a functional Advana system for TS/SCI information.[82] This lack of JWICS functionality has left customers with a sense that they cannot meaningfully engage with Advana, and has furthered the perception that data is for business analytics and not for the warfighter.

While, overall, Advana is viewed optimistically as a means of driving momentum and demonstrating data's value to skeptical commanders and warfighters, general criticism of Advana reflects a common view that the platform is a helpful tool for data-literate people but not for general or battlefield use.[83] More specific criticism of Advana highlights problems with redundant and overlapping capabilities, dissatisfaction with the platform's limited ability to write software to complete non-trivial transformations on data, missing basic functionality such as loading data that is not present in the system or code that is not in basic Python files, and issues with needing to move between multiple systems requiring different accounts to complete work.

DoD needs to transform its closed architecture, address the lack of data extensibility across environments, and mirror industry leaders who rely on large-scale AI or machine learning (ML) models accelerated via APIs. To implement an API-first approach, we recommend the following:

1. The Deputy Secretary should issue guidance demanding accountability for implementation of API-first strategies. Components should be accountable for the integration of APIs in their technology strategies. Leaders should be required to demonstrate how new technology can connect to existing systems via APIs before procurement.
2. The CDAO should be tasked to establish immediately DoD-wide API standards and technical guidance to promote

[75] DIB engagements with anonymous DoD and industry stakeholders (2023, October 27, November 17, December 1, and December 8)
[76] DIB interview with anonymous DoD stakeholder (2023, August 25).
[77] DIB interview with anonymous DoD stakeholder (2023, November 28).
[78] DIB interview with anonymous DoD stakeholder (2023, November 7).
[79] DoD stakeholders of various altitudes and backgrounds expressed this point throughout our discussions. There is an insufficient number of user interface (UI), user experience (UX), and other product design and management professionals across the enterprise, and our ability to display and enable data for non-experts is lacking.
[80] DIB interview with anonymous DoD stakeholder (2023, December 19).
[81] DIB interview with anonymous DoD stakeholder (2023, December 28).
[82] DIB interview with anonymous DoD stakeholder (2023, September 20).
[83] DIB interviews with anonymous DoD stakeholders (2023, December 18 and 19).

interoperability between different systems and platforms. Currently, Components are in various stages of developing API-first plans, but there is not uniform guidance on API integration.[84]

3. The CDAO should maintain updated API-first procurement guidelines. Modifying procurement policies and contractual language to prioritize solutions with robust API connectivity will not only streamline current operations but also ensure flexibility for future technology integrations.
4. Every CDAO should mandate API integration in their organization. All new technology acquisitions and upgrades within DoD organizations must include compatible APIs.

DoD also needs to expand enterprise capabilities in secure environments, improve the front-end user experience of these technologies, and help administer the use of data at echelon. Therefore, we also recommend to:

1. Allocate funding to hire more active TS/SCI-cleared data and AI/ML specialists to work on building the Advana JWICS environment.
2. Provide enhanced application design, user-experience development, and product management capabilities to every COCOM ADA team, where those competencies are in high demand, and then build out organic product management teams at echelon.
3. Authorize classified developer environments that software engineers can readily work in to fuel data innovation (e.g. to develop unique tools such as Gamechanger, a platform to analyze DoD policy documents and currently one of the most popular applications on Advana).
4. Provide more frequent Industry Days, e.g. for the CDAO Advana team to better integrate user requirements into the Advana platform and associated enterprise data and analytics environments.
5. Build data visualization capabilities that help capture the data organizations have, how different data sets are related, how the data is being used, and what changes are being made to that data. For example, knowledge graphs that can be combined with generative AI could enable commanders and warfighters alike to ask basic questions and receive fast and accurate feedback on their data.[85]

INCENTIVES: Change profit opportunities by updating contract incentives.

Except in a few cases (e.g. treating autonomy as a payload for future weapons systems) there are few current financial incentives for defense contractors to care about a DoD data economy. The lion's share of cash flow opportunity remains in providing platforms, ensuring they have minimal third-party upgrade opportunities, and capturing modernization and sustainment opportunities. With such platform programs currently generational, it is understandable why this "lock-in" strategy is necessary for cash flow certainty for Original Equipment Manufacturers.

For a DoD data economy to exist, there must be the *economy*: significant predictable revenue opportunities for third-party software – to include data analytics and AI – that benefit both software and platform providers alike. Apple's App Store business model, bringing in nearly a third of all app sales, is a model worth emulating for defense platforms.

Though the "economy" will take time to emerge as successive contracts must make data-focused pivots together, there are both preparatory and pathfinding opportunities each Service may begin performing now:

1. Review and Amend Current Contracts Where Feasible: Audit existing contracts to identify opportunities for integrating data-

[84] DIB interviews with anonymous DoD stakeholders (2023, August 17, October 9, November 7, and 2024, January 4).

[85] DIB interviews with anonymous DoD and industry stakeholders (2023, November 9 and December 5).

related incentives. Modify terms to include rewards for data sharing and utilization.

2. Develop New Contractual Frameworks: Create contract templates that value data access and data exploitation as key deliverables. Develop and include standard clauses for data sharing, interoperability, and exploitation.
3. Develop Pilot Programs for Data Monetization: Initiate pilot programs in different services to test new contractual frameworks. Analyze the outcomes to refine and scale best practices. Encourage "Pay for Performance."
4. Engage Stakeholders and Educate: Conduct workshops and training sessions for DoD procurement officers and defense contractors on all new data-centric acquisition practices. Update DAU curriculum and DoD websites to reflect them.
5. Monitor and Evaluation: Implement a system for the regular assessment of contract performance with a focus on data-related metrics. Focus on increasing competition and innovation in defense software development, minimizing the use of Justification and Approvals (J&As) for sole-source awards.

IMPLEMENTATION: Build service- and theater-level data capabilities at echelon.

A significant impediment to proper oversight of the DoD data economy is the haphazard placement of data chiefs within DoD Components and their associated real-world authorities and resourcing. Components correctly tasked with incorporating data leaders have not been provided with sustained, meaningful assistance in identifying, hiring, onboarding, training, integrating, and transitioning candidates for these new positions.[86] Even the naming convention for these positions varies across the enterprise; most are called Chief Data Officers (CDOs), some are called Chief Data and Artificial Intelligence Officers (CDAOs), and still others are referred to as Chief Data and Analytics Officers. Indeed, the Department of the Navy has not had a full-time CDO since the billet was abolished early last year, and its current acting CDO – a non-Senior Executive Service (SES) employee – remains nested under the Navy's Chief Information Officer (CIO).[87] The Department of the Army has a Tier 3 member of the SES who is also Army's Deputy CIO. Meanwhile, the Department of the Air Force has a Tier 1 SES who also reports to the Air Force CIO.[88] There is similar variance in the placement of CDOs and CDAOs at the COCOMs, where data leaders are often buried inside the J-codes (usually the J6).[89] These examples illustrate the discontinuity between a CDAO's statutory and real-world responsibilities, which, depending on the maturity of an organization's digital transformation, may encompass everything from modernizing infrastructure, to evolving governance practices, to ensuring information security compliance. As a result of the lack of support for organizations hiring CDAOs, Components have experienced mixed results in identifying capable data leaders for these positions and utilizing them to good effect.

For data-centricity to percolate across the Department, Component CDAOs should possess real authority over the data in their own organizations. While the DoD CDAO has pursued a decentralized approach to establish guidelines for the Department, Component CDAOs are relatively new positions that do not yet own their organizational data and have limited power to enforce these policy and procedural conditions; that authority still rests

[86] DIB interview with anonymous DoD stakeholder (2023, December 13).
[87] DIB engagement with anonymous DoD stakeholders (2023, November 17).
[88] DIB interview with anonymous DoD stakeholder (2023, November 7).
[89] DIB interview with anonymous DoD stakeholder (2023, December 18).

with each Component program office.[90] Until Component leaders push ownership of their data lakes to their CDAOs, improperly placed and utilized CDAOs have in some cases created an added layer of bureaucracy without resolving their underlying issues around data access.[91]

To build out data-centric processes within all MILDEPs, COCOMs, fourth estate defense agencies, and defense field activities, all Components should have a qualified, dedicated, standardized CDAO portfolio (i.e., a full-time, billeted SES with no other job duties and a clear portfolio encompassing data, analytics, and AI). To ensure clear accountability, all Component CDAOs should establish a memorandum of agreement with their parent organization illustrating that each CDAO should be:

1. Placed within the organization for maximum effect, e.g. as a direct report to their under secretary, commander, or director.
2. Fully empowered to make and change policy as required to implement organizational change, e.g. integrated as a topline principal within the organization.
3. Fully resourced in alignment with the 2023 *Data, Analytics, and AI Adoption Strategy* and the organization's associated Data Strategy Implementation Plan.
4. Given oversight of all "data money" throughout the organization including the authority to kill funding or disconnect systems, e.g. as the CIO has "oversight" of all IT spend.
5. Mission-oriented rather than systems- or technology-focused, e.g. not a report to a CIO or CTO-equivalent, or embedded further down in the organization.
6. Responsible for overseeing AI adoption, e.g. to ensure that data and AI efforts are fully aligned.
7. Evaluated based on clear and consolidated metrics that are standardized within executive analytic tools such as the Pulse dashboard.
8. Responsible for 100- and 500-day implementation plans to achieve practical, time-bound outcomes.

[90] DIB interview with anonymous DoD stakeholder (2023, December 18).

[91] DIB interview with anonymous DoD stakeholder (2023, December 19).

Conclusion

As an organization, DoD has fallen far behind in modeling data-centricity and facilitating data access. Industry has outpaced us by decades, incorporating data management principles across the entire lifecycle. Today, first-rate companies demand interoperability within their software; within DoD, organizations remain riddled with systems that are incapable of data integration via APIs.

Some parts of DoD have begun to incorporate modern data practices into their routine operations, but the majority of Components are failing to provide a unified approach to managing data access, sharing, and use. Data interoperability is not simply a matter of technological convenience, it is a critical underpinning of long-term operational effectiveness, and thus a strategic imperative for maintaining DoD's tradition of warfighting excellence in an increasingly data-centric global environment.

Today, DoD's ability to counter threats to national security wholly depends on informed decision-making from the boardroom to the battlefield. This report, with its initial focus on data access in collaboration with industry, will meaningfully address that mission. The DIB's recommendations in this study underscore the need to address, in short order, the fundamental cornerstone of any modern data economy: streamlined data access through immediate improvements in data interoperability across the defense innovation ecosystem, as well as longer-term changes for eroding entrenched data silos and empowering communities of young digital natives to thrive. The driving, underlying assumption of these suggested actions is that failure to adopt data best practices will degrade the force and leave our nation unprepared for future conflicts. These recommendations, taken as a whole, offer a roadmap to meaningfully advance DoD efforts to establish a robust data economy by 2025.

Appendix A – Enhancing Data Access and Interoperability in Defense Contracts: A Proposal for the FY25 National Defense Authorization Act

The Department of Defense (DoD) faces significant challenges in accessing and managing data that originates from the systems and services it develops in collaboration with industry. Prevailing data access approaches are outdated, inhibiting effective interoperability and utilization of data across various platforms to enable Combined Joint All-Domain Command and Control (CJADC2).

Recommendation: The current state of data access within DoD vendor agreements is fragmented and inconsistent, creating inefficiencies and missed opportunities for harnessing the full potential of industry data-driven solutions. The Defense Innovation Board (DIB) proposes that the next NDAA include a requirement for government contractors to enshrine DoD data access and rights in all vendor agreements. This requirement will:

1. *Secure contractual data access for DoD.*
    - Mandate DoD rights to data obtained from commercial, subscription-based platforms.
    - Claim ownership of data generated through DoD-funded commercial technologies.
    - Establish expansive rights for future data transformations and data ensembles.
2. *Set data sharing incentives for industry.*
    - Implement sophisticated data monetization methods (e.g. royalty-based licensing agreements, performance-based contracts, discount-pricing models) to incentivize industry data sharing.
    - Encourage trusted industry partners to avail their data to foster research collaboration.

Implementation: To set conditions for this data marketplace, this proposal should include:

1. *A federated data catalog for defense technology: a multi-vendor data catalog integrating data sources from across the defense industrial base enterprise.*
    - This catalog will serve as a central repository for defense technology industrial data, enhancing accessibility and interoperability between DoD industry partners.
2. *A trusted community of interest for accessing this federated data catalog: a central community comprising vendors, warfighters, and acquisition program executives.*
    - This community will facilitate collaboration on requirements, concepts of operation, and design processes, ensuring early exposure of end-users to the development phases.
3. *An independent oversight body for this new data catalog and community of interest.*
    - This body will ensure compliance with data access requirements and foster continuous improvement in data management practices.

Conclusion: Adopting these recommendations in the upcoming NDAA will enshrine data access in future DoD's contracts thereby ensuring that DoD and its industry partners are better equipped to handle the evolving challenges of modern warfare and defense operations.