DEPARTMENT OF DEFENSE

Data, Analytics, and Artificial Intelligence Adoption Strategy

Accelerating Decision Advantage
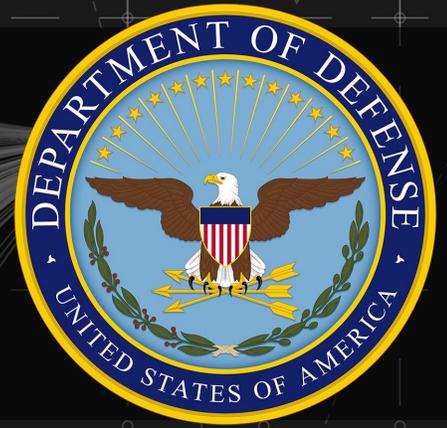
TABLE OF CONTENTS

> "America's DNA is to innovate …
> and it has repeatedly enabled us to
> drive and master the future
> character of warfare."

Kathleen H. Hicks
Deputy Secretary of Defense

FOREWORD

The Department of Defense (DoD) has been investing in artificial intelligence (AI) and responsibly fielding data- and AI-enabled systems for over 60 years. Today, data, analytics, and AI technologies are increasingly available to DoD Components and providing value to our service members.

Alongside industry's advancements, DoD has for years made steady and swift improvements to its data foundation and analytics capabilities: experimenting with AI through research and development, integrating these technologies into business and warfighting functions, and laying the foundation for their use at scale. As our investment, experimentation, and innovation continues and accelerates, our task now is to drive the diffusion of these technologies across the enterprise.

Although our strategic competitors have ambitious aims for AI, the United States and its military possess strong structural advantages in talent, warfighting experience, technology availability, and systems integration — not to mention the values that guide everything we do. Equipping our people with the tools and resources to make better decisions faster will increase the efficiency of DoD business operations, make our warfighting capabilities and the people who command them more effective, and create opportunities to employ novel operational concepts.

Responsibly and rapidly realizing the full promise of data, analytics, and AI is not the sole job of a single organization or program; it's on all of us. Providing DoD data as an enterprise resource, for instance, requires more sharing and collaboration, not less. We seek an agile strategic approach that guides decentralized action across DoD, inspires campaigns of learning, and leverages all our people, processes, and enabling technologies.

As we have integrated analytics and AI applications, we have observed their benefits and learned crucial lessons about their limitations. From the boardroom to the battlefield, more work remains, such as improving data quality and network infrastructure. This Strategy serves as a guide for how we will strengthen the organizational environment in which DoD deploys data, analytics, and AI capabilities for enduring decision advantage.

Successfully defending the nation depends on our people. As we have always done, DoD will continue to trust, support, empower, and invest in our people. We will not outpace our adversaries through imitation. We will succeed by leading with our strengths: our democratic values, our diverse and open society, our culture of ingenuity, our second-to-none innovation base, and our globe-spanning network of Allies and partners. Together, we will harness data, analytics, and AI for the defense, security, and prosperity of the American people and the world.

Kathleen H. Hicks
Deputy Secretary of Defense

STRATEGIC ENVIRONMENT

As the 2022 National Defense Strategy (NDS) makes clear, the United States possesses strengths that our competitors cannot match, among them our diverse and open society, our culture of ingenuity, our innovation base, and our globe-spanning network of Allies and partners. The Department leverages these strengths by distributing authority, empowering leaders in our All-Volunteer Force to innovate at the edge and apply their own judgment to combine old and new capabilities into superior operational concepts. The latest advancements in data, analytics, and artificial intelligence (AI) technologies enable leaders to make better decisions faster, from the boardroom to the battlefield. Therefore, accelerating the adoption of these technologies presents an unprecedented opportunity to equip leaders at all levels of the Department with the data they need, and harness the full potential of the decision-making power of our people.

The NDS also describes the need for the United States to sustain and strengthen deterrence against the People's Republic of China and other strategic competitors, which have widely communicated their intentions to field AI for military advantage. Accelerating adoption of data, analytics, and AI technologies will enable enduring decision advantage, allowing DoD leaders to prioritize investments to strengthen deterrence; link cross-cutting campaign outcomes that counter our competitors' coercive measures; and deploy continuous advancements in technological capabilities to creatively address complex national security challenges in this decisive decade.

The urgency of the strategic environment and the scale at which the Department must operate are formidable. The Department is well-positioned to excel because it has established a foundation of strategic guidance informed by lessons learned from hands-on initiatives over the last several years.[1] The Department's first AI Strategy, published in 2018, and revised Data Strategy, published in 2020, are two of these foundational efforts. The 2018 AI Strategy emphasized the need to build centralized infrastructure for AI development, to bridge AI technology developments from the Department's research and engineering communities, and to exercise international leadership in military ethics and AI safety. The 2020 Data Strategy envisioned the Department as a data-centric organization that can employ data supporting advanced capabilities for operational advantage and increased efficiency, and oriented enterprise data management activities toward the VAULTIS goal framework.[2]

1. This guidance includes the DoD AI Strategy (2018), the DoD Digital Modernization Strategy (2019), the DoD Data Strategy (2020), the DoD Enterprise DevSecOps Strategy Guide (2021), the DoD Software Modernization Strategy (2022), the Trusted AI and Autonomy Critical Technology Roadmap (2022), and the DoD Zero Trust Strategy (2022).

2. The 2020 DoD Data Strategy outlined the following seven goals (VAULTIS): *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.

Since these strategies were published, industry has produced more tools, platforms, and services for federated environments, enabling more effective, decentralized data management, and analytics and AI development. Adoption of these commercial offerings has allowed organizations within the Department to focus on necessary internal transformation efforts and deploy government-owned tools, services, and platforms for military use cases. The Department has matured collaboration with academia, industry, as well as Allies and partners, and promoted best practices on data management, responsible AI, and AI readiness. Experimentation and fielding have resulted in a deeper understanding of the degrees of data quality and availability required to develop and deploy advanced analytics and AI capabilities at scale.

This DoD Data, Analytics, and AI Adoption Strategy builds upon and supersedes the 2018 AI Strategy and the 2020 Data Strategy to continue the Department's digital transformation. The Department will continuously seize opportunities presented by iterative technology advancements, at the speed of relevance and at the scale of our global mission. To do so, the Department requires a unified approach across data, analytics, and AI activities; an educated, empowered workforce skilled at incorporating commercial teams and tools; continued advanced research and rapid experimentation; and effective integration with our Allies and partners. The Department cannot succeed alone. Our integration of data, analytics, and AI technologies is nested within broader U.S. government policy, the network of private sector and academic partners that promote innovation, and a global ecosystem. We need a systematic, agile approach to data, analytics, and AI adoption that is repeatable by all DoD Components. This strategy outlines our approach to improving the organizational environment within which our people can deploy data, analytics, and AI capabilities for enduring decision advantage.

KEY OUTCOMES

As a result of implementing this strategy, DoD leaders and warfighters will be able to make rapid, well-informed decisions by expertly leveraging high-quality data, advanced analytics, and AI as part of a continuous, outcome-driven, and user-focused development, deployment, and feedback cycle.

The Department's investments in data, analytics, and AI will address key operational problems identified in the 2022 NDS, fill validated gaps to enhance the warfighting capabilities of the Joint Force, and strengthen the enterprise foundation required to sustain enduring advantages. Fielding data, analytics, and AI capabilities across this continuum from the boardroom to the battlefield recognizes that warfighting decision advantage is enabled by hundreds, or thousands, of decisions made by personnel and program offices at great distances from the frontline. Strengthening decision advantage for the Department's warfighting and business operations is key to maintaining a resilient future force that can address a broader array of operational problems, dynamically campaign and deter, and prevail in conflict, if necessary.

Decision advantage is a competitive condition characterized by the following outcomes:

- Battlespace awareness and understanding
- Adaptive force planning and application
- Fast, precise, and resilient kill chains
- Resilient sustainment support
- Efficient enterprise business operations

Agile, user-focused, product-centric development is essential to achieving these outcomes because humans and machines will work together in the responsible, effective employment of data, analytics, and AI-enabled capabilities.

Today, there are multi-disciplinary teams throughout the Department that leverage common technology development best practices. These practices include:

- Employing Agile development fundamental principles and approaches
- Building intuitive interfaces to accelerate human adoption of new technology
- Developing products with cross-functional teams focused on customer needs
- Offering product portfolios with shared digital foundations
- Experimenting with minimum viable products in operational environments to identify new concepts for use, improve capability, and manage emergent risks

More is needed now, and at scale. The Department will pursue a multi-disciplinary approach and implement these best practices to strengthen its technology, human capital, processes, and culture. This approach has implications analogous to pivoting from a heavy armor force to one with greater maneuverability. *The Department will enhance its competitive edge through a vigorous and continuous capability delivery pipeline that can respond with agility to changing environments and technologies.*

The Department's *agile approach* to adoption (Figure 1) ensures a tight feedback loop between technology developers and users through a continuous cycle of iteration, innovation, and improvement of solutions that enable decision advantage. Practicing agility and learning by doing will accelerate deployment speed–measured in hours or days, not months or years. Creating effective, iterative feedback loops among developers, users, subject matter experts, and test and evaluation (T&E) experts will ensure capabilities are more stable, secure, ethical, and trustworthy.
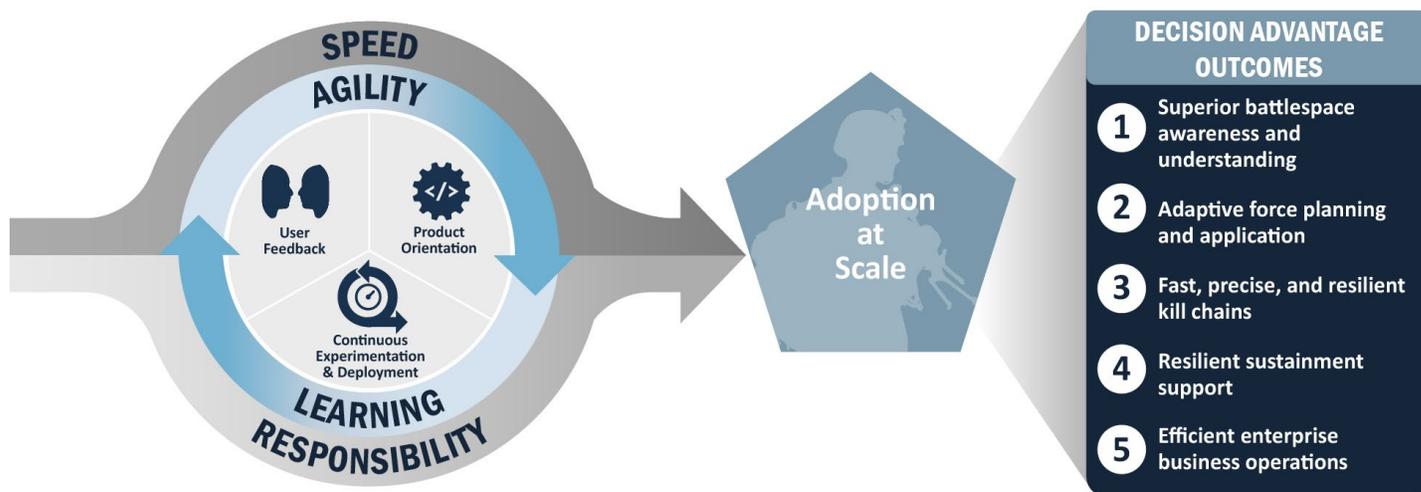

Figure 1: Employing an Agile Approach to Adoption to Scale Decision Advantage Outcomes

An agile approach to adoption emphasizes *speed* of delivery and continuous improvement, prioritizing outcomes over processes. Valuing speed necessitates organizational *agility* and *learning* through early and ongoing real-world feedback. The Department will move toward greater integration, transparency, and knowledge sharing across organizational boundaries. Increased diffusion of data, analytics, and AI technologies will introduce technical vulnerabilities that require rigorous protection measures. *These risks will be managed not by flawless forecasting, but by continuous deployment powered by campaigns of learning.* Developing capability in this way enables *responsibility*, ensuring not only the sustained quality, stability, and security of DoD systems, but also providing the means by which engineers can reduce unintended bias and instill justified confidence with their users.

The Department's agile approach to adoption ensures a tight feedback loop between technology developers and users through a continuous cycle of iteration, innovation, and improvement of solutions that enable decision advantage.

STRATEGIC GOALS

The Department will focus strategic efforts on several interdependent goals that support the DoD AI Hierarchy of Needs (Figure 2). The AI Hierarchy of Needs is a pyramid with quality data as its foundation since all analytic and AI capabilities require trusted, high-quality data to support decision makers. The next layer in the Hierarchy is insightful analytics and metrics, the foundational models and visualizations required for DoD leaders to understand their domain and the key variables impacting outcomes in those domains. At the top of the pyramid is Responsible AI, the Department's dynamic approach to the design, development, deployment, and use of AI capabilities in accordance with the DoD AI Ethical Principles while delivering better, faster insights and improved mission outcomes.[3] The layers of the Hierarchy are supported by robust sets of processes. Increased data quality and insightful analytics are achievable through effective enterprise data governance. Sound assurance processes for testing, evaluation, validation, and verification are imperative for Responsible AI. Around the pyramid are enablers, such as digital talent management, that help sustain the Hierarchy of Needs.
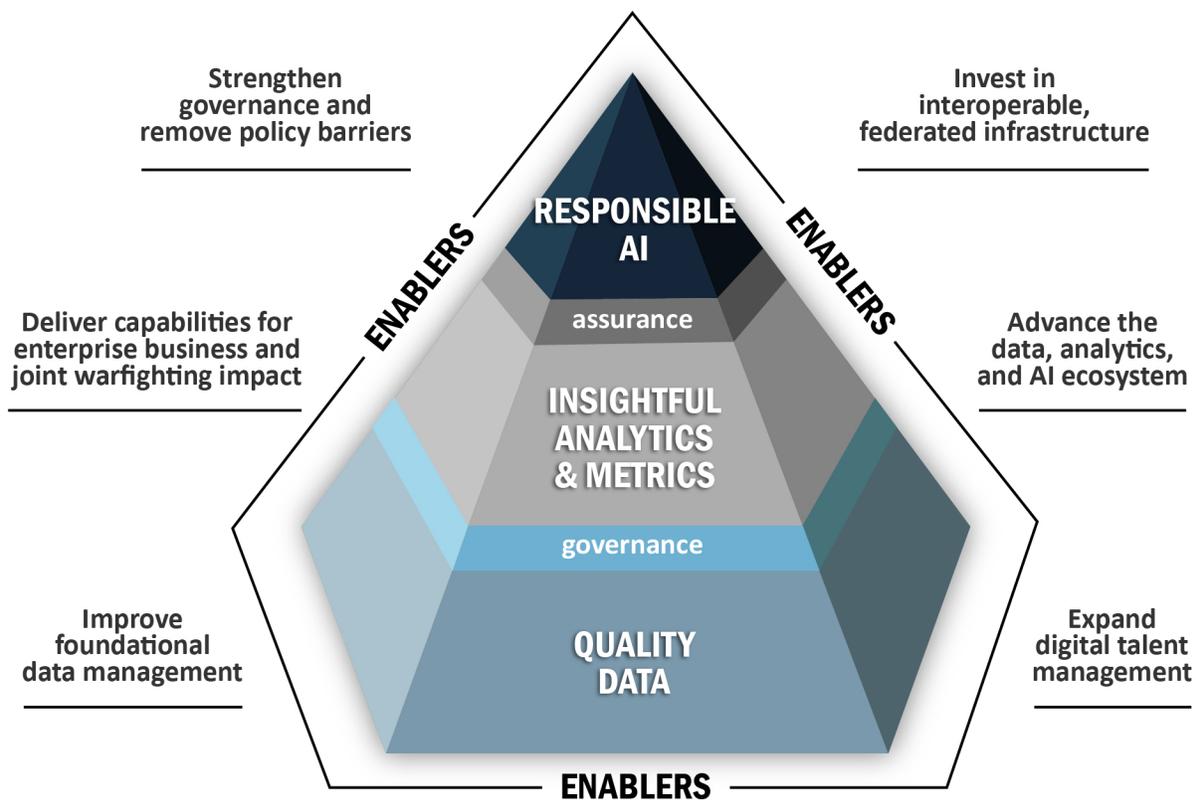

Figure 2: Strategic Goals and the AI Hierarchy of Needs

The Hierarchy is helpful as a framework for assessing DoD AI readiness, and for guiding the Department's goals to accelerate adoption of data, analytics, and AI technologies to build enduring decision advantage. These interdependent goals, and their supporting activities and investments, cut across technology, human capital, process, and culture areas, and are described in further detail on the next few pages.

3.   For more information on the Department's Responsible AI plan, see the "US Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway."

Consistent with the Deputy Secretary of Defense's Memorandum on Creating Data Advantage, the Department will value data as a product, ensuring the responsible collection, storage, and management of relevant data to support enterprise needs. All DoD data is an enterprise resource. The Department will adapt and implement open standard architectures while abiding by existing DoD cybersecurity policies and heed industry best practices for data ethics, data protection, and design as technology evolves. The Department will also continue to make its data more *visible*, *accessible*, *understandable*, *linked*, *trustworthy*, *interoperable*, and *secure* (VAULTIS). Components will assess their data across lifecycles using the data quality dimensions and the VAULTIS framework first outlined in the 2020 DoD Data Strategy.[4]

The Department's data management focus will initially prioritize improving data quality and managing data as a product in support of the Secretary of Defense's priority areas. To improve DoD data quality across the enterprise, the Department will develop and implement a decentralized network among data providers and users. This network will consist of both process-based and technical components, distributing ownership across data domains and treating data as a product. Instead of designating a centralized data team responsible for managing all data across the enterprise, data domain owners and data product teams will be responsible for managing the data products they own and produce.

Data products will be designed, built, and maintained with the needs and requirements of its users in mind, just like a traditional product. By treating data as a product, DoD Components can stimulate a culture of data sharing and reuse under appropriate circumstances, which breaks down data silos and promotes cross-functional collaboration. This product orientation ensures that data is properly managed and governed, with clear accountability, quality and interface standards, and access controls. While this data management approach will not reduce DoD's organizational complexity, over time it will improve operational and analytical data quality, reduce data backlogs, lower data storage costs, and reduce data redundancy. These improvements will allow DoD organizations to better leverage their data products and make more effective, data-driven decision-making.

4.   See Appendix A for further detail.

DELIVER CAPABILITIES FOR ENTERPRISE BUSINESS AND JOINT WARFIGHTING IMPACT: Enhance and/or generate business analytics and warfighting capabilities with data, analytics, and AI technologies for improved decision advantage outcomes

An integrated, agile approach with a strong focus on data quality will ensure the Department fields responsible solutions that most appropriately address organizational needs. There is an urgent need to surge digital support to address Joint capability gaps at the operational to strategic levels in direct support of operational commands. Building momentum toward transformation requires demonstrating tangible, near-term results. For example, a user requesting an advanced decision support model with recurring excursion capability could field a simpler analytics dashboard in the near-term to better understand current state and shape more sophisticated questions. The Department will continue to focus on advancing business analytics, to continuously improve data quality through use, and to provide the more complete picture DoD personnel need to make better reactive and proactive decisions.

The Department will design and test analytics and AI-enabled solutions side-by-side with stakeholders, business and warfighter, and demonstrate capabilities via robust campaigns of learning to account for different operational environments. Some users may have access to abundant data and high-speed processing while other users face limited bandwidth at the tactical edge. Designers will identify these constraints early in the development process. The Department will conduct continuous experiments, and integrated multi-lateral exercises with high-impact Joint Force use cases that can inform additional investments in interoperable enterprise-level, warfighting capabilities. Components will advocate for investments in data, analytics, and AI that will generate these capabilities. Capabilities deemed successful after rigorous testing will receive clear pathways to sustainment and wide-scale adoption.

STRENGTHEN GOVERNANCE AND REMOVE POLICY BARRIERS: Ensure responsible behavior, processes, and outcomes while accelerating the pace of adoption for data, analytics, and AI technologies across the Department

The Department's approach to integrated data, analytics, and AI governance will account for the scale of the organization, its distributed authority structure, and high degrees of variance in data maturity among Components. Further, the Department's information enterprise is vast and global, with strong dependencies among different IT systems, support teams, programs, and activities. For example, a key pillar of the 2022 DoD Zero Trust Strategy hinges upon the establishment of effective enterprise data governance, and the fielding of analytics and AI to secure our networks, applications assets, and services. Similarly, records management processes and procedures are another dependency. The 2023 DoD Records Strategy makes clear that records are data and will be curated, automated, and governed. Treating records in this way will increase trust in data and analytics products.

These examples of dependencies underscore the complexity of the Department's policy environment and the necessity of consensus building. The DoD data, analytics, and AI leadership community will build consensus around responsible development practices that enable mission owners and other governance bodies while serving as a demanding customer of enabling capabilities. Data, analytics, and AI governance will be risk-adjusted, streamlined, and data-driven, and focused on collaborative learning. *Generating consensus and collaboration is critical to mitigating known and emergent policy barriers and aligning technical interfaces to hasten responsible adoption.*

In support of a collaborative approach to enterprise governance, DoD Components will identify clear leaders for data-related transformation, strengthening accountability across the Department. Enterprise-level governance initiatives will prioritize key areas including data management, cybersecurity, requirements, joint interoperability, records management, and Responsible AI. The success of these areas requires Components to continue to follow responsible security procedures, review current policies and processes on data aggregation and classification, revise issuances as needed, and comply with updated guidance. The Department will approach reforms with *speed* and *responsibility*: targeting identified policy revisions to improve agility, speed of capability deployment, and scalability; while upholding a steadfast commitment to lawful and ethical behavior; and protecting privacy and civil liberties. Components' efforts to implement this Strategy will be supported by governance policies, processes, and structures that are mission-driven, responsive to need, minimally prescriptive, and based on best practices. The Department will reduce institutional barriers, including those that unnecessarily inhibit collective research and development, planning, interoperability, intelligence, and information sharing. The Department will lead across the U.S. government to inform technology and information release processes, expand release authorizations, and redefine dissemination controls to facilitate information exchange for mutual benefit.

INVEST IN INTEROPERABLE, FEDERATED INFRASTRUCTURE: Optimize the Department's federated infrastructure to support scaling data, analytics, and AI adoption and improve interoperability.

The Department will invest in abundant, flexible, secure, and jointly interoperable infrastructure that is scalable for the needs of users. Data, analytics, and AI capability development requires tremendous computing power and demand will grow exponentially as adoption scales. When appropriate, this infrastructure will be automated, including measures to implement DoD technology policies (e.g., Continuous Authorization to Operate), its status reporting, and, critically, user access to mission- relevant data, analytics,

BALANCING TRADEOFFS WITH SHARED SERVICES

COMMONALITY OF OUTCOMES

Decentralized
- Specialized requirements
- Local control/ownership
- Speed
- Local expertise and responsiveness

Centralized/Shared
- Generalized/joint requirements
- Economies of scale
- Interoperability
- Consistency and harmonization

COMPLEXITY OF IMPLEMENTATION

Figure 3: Balancing Tradeoffs with Shared Services

and AI platforms. Though government-led and designed, DoD infrastructure will adopt open standard architectures for industry and trusted partners to facilitate collaborative and continuous experimentation. As described in the DoD Software Modernization Strategy, the Department is an "enterprise of enterprises." Thus, the Department's infrastructure supporting data, analytics, and AI technologies will remain federated. The Department will continue to centralize some decisions and services while others remain decentralized to address unique mission needs. To strike the optimal balance of platforms and services, the Department will assess infrastructure based on outcome commonality and implementation complexity (depicted in Figure 3).

While it is important to strive for enterprise scaling economies, leaders must also understand the extent to which their Component's data, analytics, and AI requirements are truly specialized. Organizations with common digital service requirements and joint use cases, particularly when migration would be relatively simple, will move quickly to adopt shared services to meet their needs. Organizations' infrastructure must remain decentralized if they have highly specialized requirements or if leaders determine that the costs outweigh the benefits of consolidating within a shared platform or suite of services. One notable exception to this logic is AI-specific infrastructure. The scarcity of expertise required to customize safe and reliable AI-enabled systems remains a limiting factor. Thus, DoD Components will seek to centralize certain AI development platforms for continuous experimentation and deployment, and then maximize the adoption of responsible AI shared services.

ADVANCE THE DATA, ANALYTICS, AND AI ECOSYSTEM: Strengthen intergovernmental, academic, industry, and international partnerships to enable adoption of data, analytics, and AI technology.

The Department will advance progress toward a robust national and international ecosystem that facilitates improved intergovernmental, academic, industry, and international collaboration on data, analytics, and AI technology. *The Department cannot succeed alone.* Through domestic and international engagements, the Department will collaborate on common challenges, further shared interests, promote democratic norms and values, and increase interoperability with partners. The Department will cooperate with Allies and partners to leverage comparative advantages and allow for interoperability in tactics, institutions, and strategies related to data, analytics, and AI. Where appropriate, the Department will continue exporting key technologies and sharing data to ensure our Allies and partners remain agile and capable of rapidly employing advanced analytics and AI innovations.

To obtain and integrate proven solutions in collaboration with industry, the Department will follow an "adopt-buy-create" framework aligned with the DoD Software Modernization Strategy and Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*.

DoD leaders will first seek to adopt solutions that are already Joint- or Component-sponsored before exploring capabilities available on the open market. When DoD-owned shared services are unavailable, the Department will challenge vendors to solve specific business and mission problems, while designing acquisition strategies to avoid vendor lock-in. DoD customers with clean, high-quality data can seek commercially available analytics and AI capabilities while retaining appropriate data rights. Government contracts for commercial solutions will ensure the Department's capability pipelines address evolving requirements while balancing protection of industry intellectual property. Commercial solutions may not meet all mission requirements, but they can provide best-in-class capabilities for many dual-use applications. It is often in the Department's interest to procure software and support for these commercial solutions, freeing up DoD engineers for inherently governmental challenges. Fielding web-based, cloud-based, and/or Application Programming Interface (API)-first applications create more opportunities for rapid, enterprise scalability; continuous integration and delivery; and increased economies of scale. APIs also allow for a more open exchange with diverse data sources, regardless of origin, giving DoD leaders and warfighters greater access to the information they need to make more timely and accurate decisions.

The Department will only create solutions when those applications aid DoD-specific missions and cannot be readily adopted from commercial or existing solutions. These Defense-specific applications often involve real-time, mission-critical, embedded software coupled to customized DoD hardware. Creating an ecosystem that fosters competition and collaboration is essential for the development and deployment of AI-enabled systems, particularly next generation capabilities for use in Joint warfighting. When supported with open standard architectures, the Department's data, analytics, and AI ecosystem will facilitate commercial competition based on model performance and promote collaboration with trusted international and intergovernmental partners. Commercial models verified, validated, accredited, and fielded through this process can then be customized for DoD use.

Program managers will consider acquisition strategies that leverage international partnerships and supportability planning to improve economies of scale, strengthen the defense industrial base, and enhance Ally and partner capabilities. Further, the Department will embrace initiatives aimed at creating standard language necessary for data, analytics, and AI technology contract problem statements and agreements. When applicable, the DoD will leverage resources such as the federated data and model catalog and AI-enabled enterprise tools to expedite acquisitions. The Department will mature and expand acquisitions policies that increase government visibility of the ownership, labeling, maintenance, and classification of data. The Department has made progress on acquisition innovation and will continue to encourage personnel to embrace risk and learn by doing. Contracting must be as agile as the industry with which it is engaging. The Department will continue to adapt best practices from nontraditional partners to ensure cutting edge solutions are delivered responsibly at the speed of relevance.
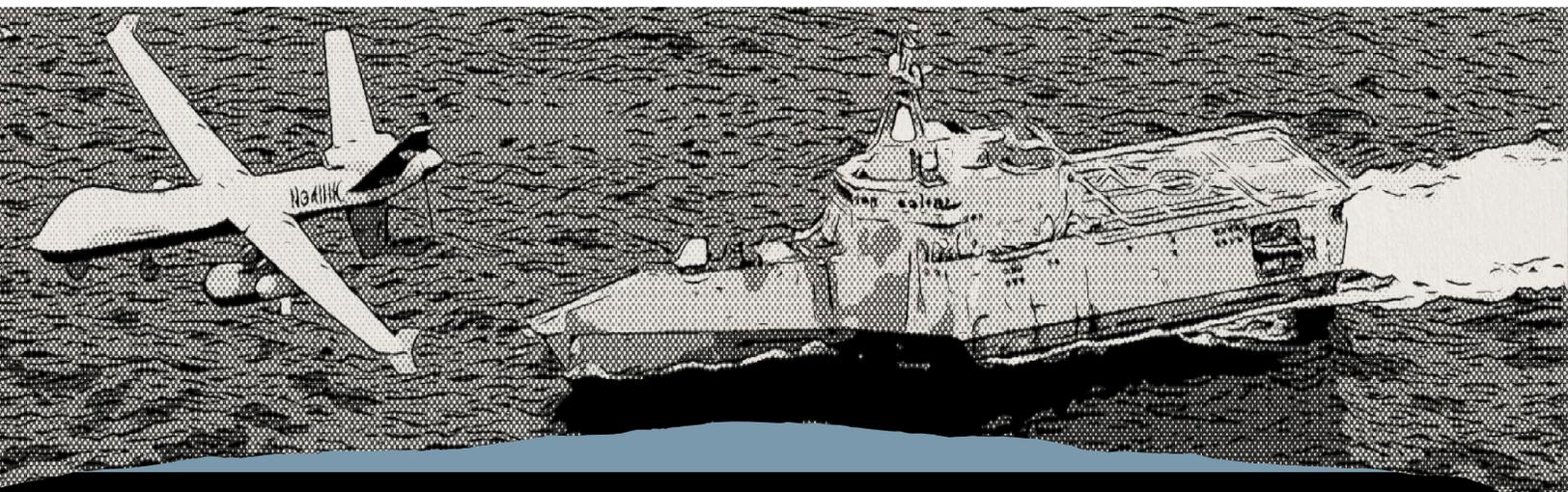
EXPAND DIGITAL TALENT MANAGEMENT: Increase hiring, training, and retention for the most critical data, analytics, and AI-related work roles.

The Department's ability to oversee and adopt data, analytics, and AI capabilities depends on the strength of its workforce, and continued growth in technical skills. The Department will ensure it is identifying and employing the talent it already possesses, then focus resources on those initiatives and tools that best attract, recruit, train, and retain a truly innovative workforce across digital talent work roles. The Department will also identify and train nontechnical personnel who will lead and oversee a culture of innovation that advances the responsible use and adoption of data, analytics, and AI capabilities.

The Department's infrastructure and digital ecosystem remain obstacles to hiring talent from the cutting edge of the private sector. While the Department takes all necessary steps to enhance its technical foundation, talent management efforts and resources will focus on upskilling and reskilling Service members and civilians in the work roles that DoD Components have determined are the most important for addressing the needs of the Department. For instance, Service members and civilians with domain knowledge and basic digital skills will be upskilled or reskilled with targeted training and hands-on opportunities to serve in work roles such as data architect, data steward, and user experience designer within the newly expanding Department-level workforce framework.

Components will draw personnel identified for upskilling and reskilling opportunities from the Department's Total Force. Active and Reserve Service members often possess high-demand digital skills not directly aligned to their occupational specialty. To retain talent, the Department will create more flexible service structures that cultivate and reward strengths and avoid penalizing personnel for selecting non-traditional career paths.

While the DoD digital workforce grows and strengthens through upskilling and reskilling, the Department will also think differently about maturing pipelines to attract, recruit, and flexibly hire digital talent. Components will use existing hiring authorities and retention tools at their disposal, and institute reforms where appropriate to allow for maximum flexibility in garnering digital talent. Additionally, the Department will execute a series of pilots to identify organic talent, validate barriers and blockers presented, and establish a cadre of Service members and civilians from across the DoD enterprise to build and apply digital solutions for the most difficult missions.
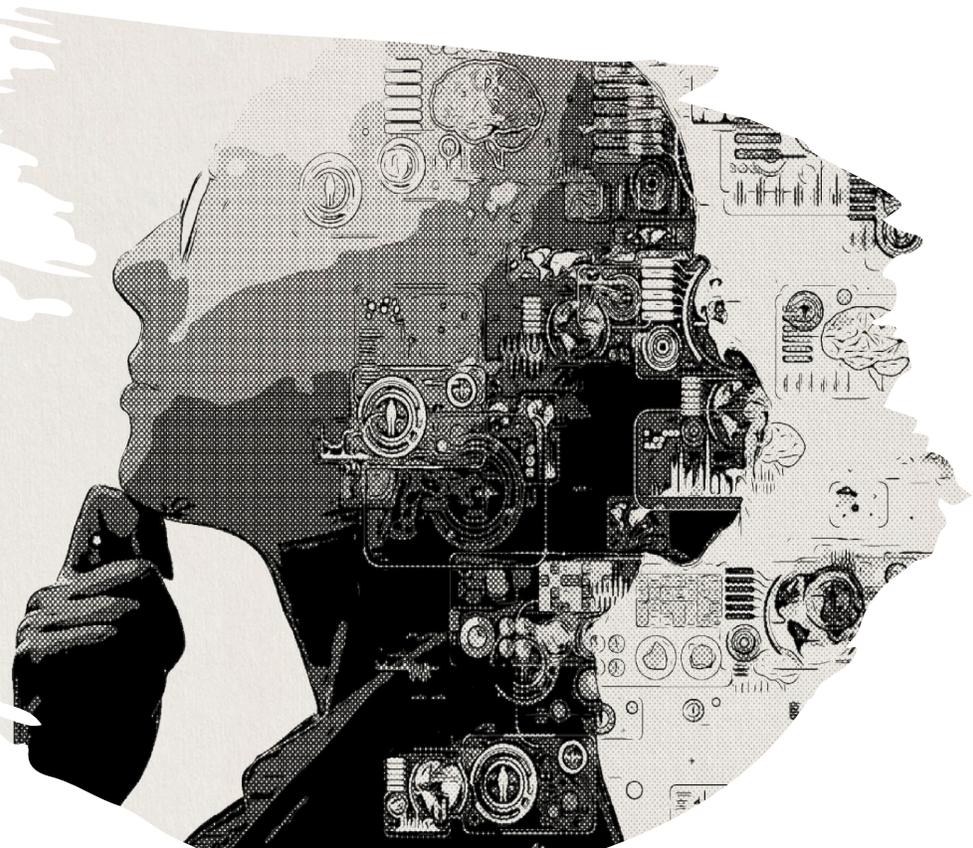
IMPLEMENTATION

The Chief Digital and Artificial Intelligence Office (CDAO) will lead and oversee the implementation of this Strategy. The CDAO will collaborate on implementation with Components through the CDAO Council, the senior leadership body that governs and coordinates the Department's integrated data, analytics, and AI enterprise.[5]   For certain issues, the CDAO Council recommends decisions on data, analytics, and AI to the Deputy's Management Action Group, the Deputy's Innovation Steering Group, and the Deputy's Workforce Council. The CDAO will conduct an annual review of the Strategy and report results through the CDAO Council. The CDAO Council and supporting forums will ensure the exchange of challenges, lessons, and best practices gleaned from across the Department, and oversee initiatives for digital talent development, leadership, and culture as critical enablers.

IMPLEMENTATION PLANNING GUIDANCE

DoD Components have assigned oversight for data, analytics, and AI differently based on their missions, governing laws and applicable procedures, and organizational structures. The state of data maturity across the Department varies significantly from Component to Component. Thus, Components will tailor implementation according to self-assessed data maturity levels, mission parameters, and pertinent laws. This strategy does not prescribe that Components reorganize in the same fashion as the DoD CDAO. However, within 60 days of publication, Components will designate their team or office of primary responsibility for implementing this strategy and identify any teams or offices with contingent responsibilities. After analyzing the goals of this strategy, Component leaders may determine that multiple teams will be responsible for implementation.

Based on lessons learned from implementing the previous DoD AI and Data Strategies, outcomes-based performance indicators will be established, refined, and monitored in coordination with the CDAO Council as an integrated part of the Department's enterprise performance analytics framework. To further aid Component-level decision-making and execution, the CDAO will publish expanded implementation guidance and additional appendices to this strategy. The expanded implementation guidance will outline the process by which the CDAO and CDAO Council collaborate with the Components to create agreed upon strategic performance measures linked to this Strategy's key outcomes and strategic goals. This collaborative process will ensure measures are supported by authoritative data sources and maximize the use of automated data collection methods for efficient performance monitoring. Where Authoritative Data Sources do not exist, the CDAO will assist in their construction and maturation until these sources meet senior leader decision requirements.

RISK MANAGEMENT

Data, analytics, and AI-enabled technologies are having profound impacts on the ways we work, live, and engage with one another. Aided by training and user-friendly interfaces, the integration of these capabilities within the Department's systems and activities will continue to increase until they are nearly ubiquitous. The anticipated breadth of adoption by the Department and its competitors, and the nonlinear evolution of these technologies, present strategists with unique foresight challenges, especially for resource planning. For data, analytics, and AI technologies, Components will identify and adopt resourcing schemes, processes, and assessment tools that offer leaders maximum flexibility to compliantly deliver iteratively developed capabilities at speed. Each iteration or release cycle will incrementally reduce risk while rapid feedback loops ensure that Components more consistently meet user demands. By staying adaptive, the Department can maintain a deep understanding of the specific needs of end users and adjust more quickly to changes in the security environment.

This strategy's learning-based, agile approach to adoption and emphasis on data quality also mitigate implementation risks. Though strategic success depends upon a high degree of decentralized execution, the CDAO Council and Component leaders can learn from one another and coordinate to manage critical dependencies among the goals in this strategy and parallel goals in other DoD strategies. As the warfighting use cases for analytics and AI technologies continue to expand, we can expect our strategic competitors to field them to enhance their capabilities. Our adversaries will also continue to target U.S. technologies for theft and exploitation. Therefore, the Department will employ development approaches that allow us to move quickly, protect our advantages, and abide by our laws, policies, and values. The Department recognizes the privacy and civil liberties challenges posed by data, analytics, and AI capabilities and will establish transparent governance and compliance processes that address the full scope of these potential risks. By focusing on data governance and data quality for analytics and AI development, the Department can mitigate certain risks, including the replication of unintended bias across the enterprise. Component leaders and technologists remain committed to the objectives of the DoD Responsible AI Strategy & Implementation Pathway and to developing AI capabilities that are *responsible*, *equitable*, *traceable*, *reliable*, and *governable*.

CONCLUSION

The Department's scale and warfighting mission are unique, but organizations from all sectors have overcome similar challenges and have harnessed the benefits of digital transformation. DoD leaders will have access to high quality data, advanced analytics, and AI capabilities to make timely and well-informed decisions to defend the homeland, deter aggression, and win in conflict. Our military competitors are integrating these same technologies for their own advantage. We cannot afford to wait and, moreover, we cannot succeed alone. This strategy's approach embraces the need for *speed*, *agility*, *learning*, and *responsibility*. Pursuing this agile approach and focusing activities on the goals outlined in this strategy will allow the Department to adopt data, analytics, and AI-enabled capabilities at the pace and scale required to build enduring decision advantage. If we confront our challenges holistically and refuse to accept the status quo, we *will* accelerate data, analytics, and AI adoption and continuously deploy creative solutions for the defense, security, and prosperity of the American people.
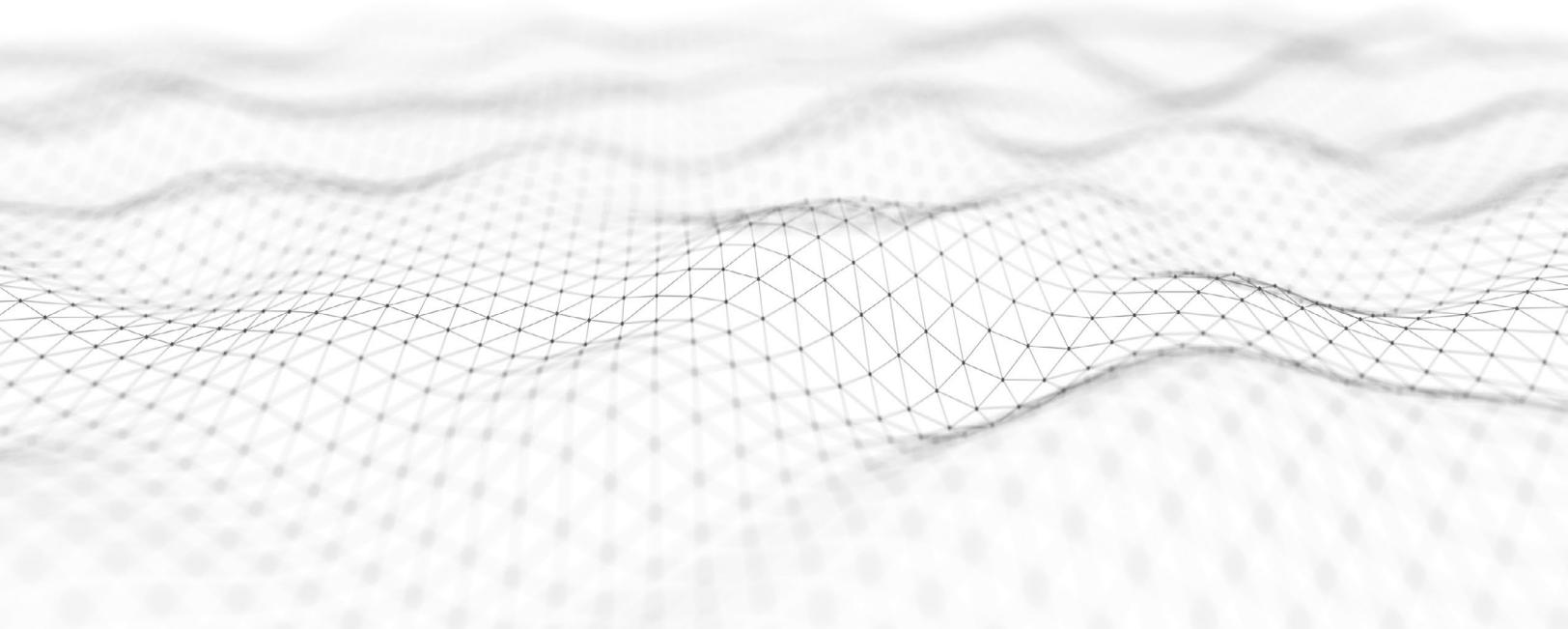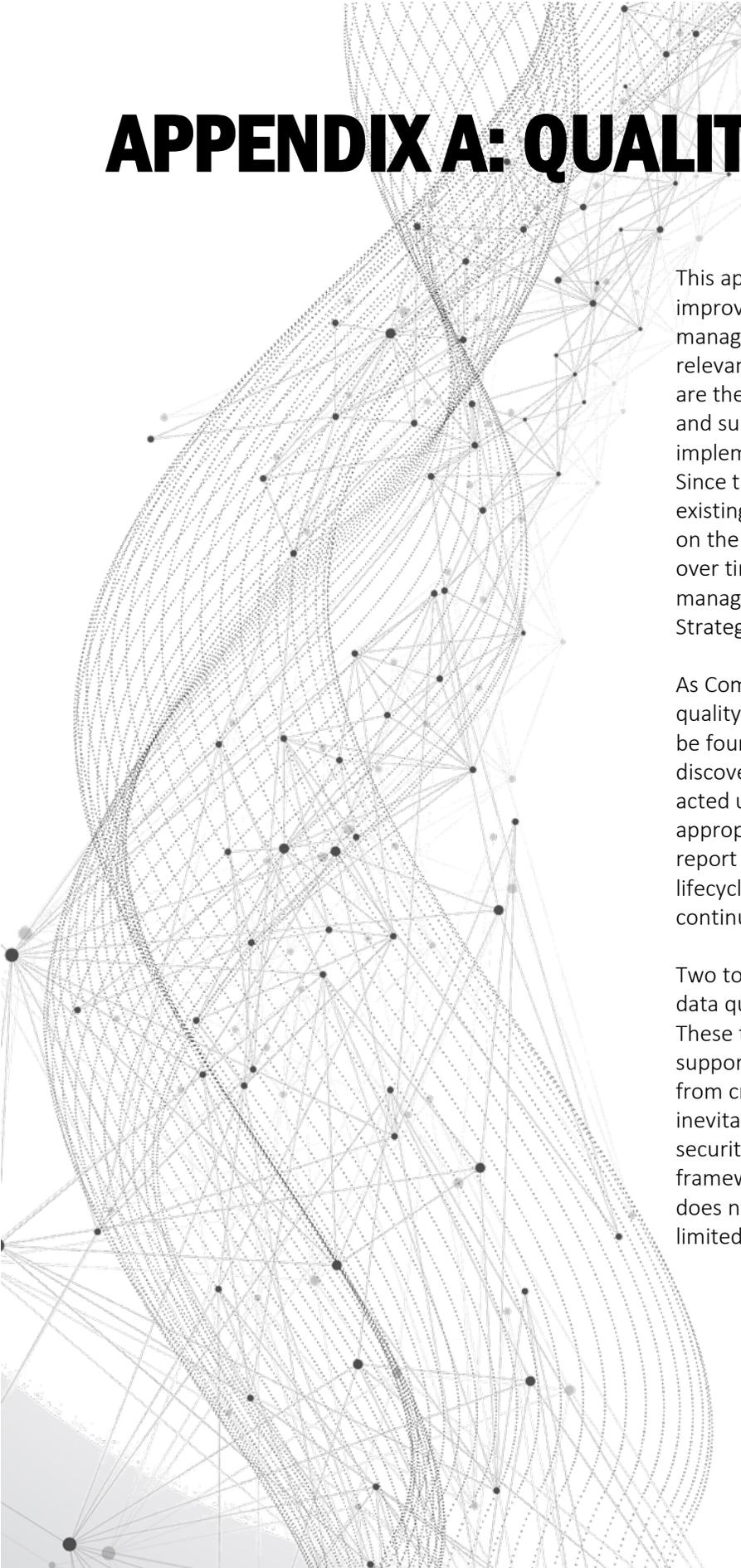
APPENDIX A: QUALITY DATA

This appendix provides additional guidelines for improving the Department's foundational data management to increase the quality and availability of relevant DoD data. User needs and local requirements are the basis of data quality. Therefore, Components and subordinate organizations will develop data quality implementation guidance and associated metrics. Since this appendix retains the VAULTIS framework, existing Component-level implementation plans based on the 2020 Data Strategy are still sound. However, over time, Components will evolve their data management plans to align more closely with this Strategy.

As Components develop and implement their data quality plans, data sets targeted for improvement will be founded on metadata to allow for data search and discovery; prioritized for relevance and mission value; acted upon such that improvement efforts are appropriately resourced; monitored to measure and report quality levels on priority data sets across their lifecycles; and corrected through cyclical processes to continuously address quality degradation.

Two tools for use in data management planning are the data quality dimensions and the VAULTIS framework. These tools represent interrelated and mutually supporting concepts that apply across data's lifecycle, from creation to disposal. Poor quality data will inevitably undermine data trustworthiness, raise security concerns, and negate the utility of the VAULTIS framework. Conversely, even high-quality data that does not align to the VAULTIS framework will be of limited value to analytical and AI efforts.

1. DATA QUALITY DIMENSIONS

Data owners may categorize data sets at different levels of quality over time because of age, prioritization, initial condition, and other factors. Therefore, data quality dimensions are relative, and owners will assess the dimensions across the data's lifecycle. The table below provides sample assessment questions for each dimension.

Dimension	Assessment Questions
Accuracy: Data that correctly reflect proven, true values or the specified action, person, or entity. Accuracy includes data structure, content, and variability.	❑ How frequently do values not align to their assigned format? ❑ How frequently do data values match ground truth? ❑ How is error measured? Is it tolerable for the specified purpose?
Completeness: The data present at a specified time contain the expected information or statistics, as measured at the data set, row, or column level.	❑ Is there known data that would make the set more complete? ❑ Does the data set contain sufficient breadth of information to contextualize the data for its purpose? ❑ What fields in the data expect some null values? How often are null values present?
Conformity: Data sets follow agreed upon internal policies, standards, procedures, and architectural requirements.	❑ Does the data's format match the applicable standard(s)? ❑ Is the data set architecture published and available? ❑ Are there database constraints implemented in accordance with internal policies, standards, and procedures to prevent erroneous input?
Consistency: The degree to which a value is uniformly represented within and across data sets.	❑ Are there other data sets that reference values in this data set? ❑ Are there discrepancies?
Uniqueness: Ensures there is a one-to-one alignment between each observed event and the record that describes such an event.	❑ Are there other Authoritative Data Sources that serve the same function? ❑ Are there duplicate records in this data set?
Integrity: A data set's pedigree, provenance, and lineage are known and aligned with relevant business rules.	❑ Are there opportunities for data to be tampered with, misreported, degraded, corrupted, poisoned, or otherwise altered during the collection, storage, processing, or transmission processes? ❑ How often are data quality checks conducted to address poor data quality? ❑ Does the data cleaning process result in data that can be trusted?
Timeliness: Measures the time between an event occurring and the data's availability for use.	❑ How frequently do supported data consumers require updates? ❑ Does the data purpose require reduced latency?

2. VAULTIS FRAMEWORK

The VAULTIS framework discussed in the 2020 DoD Data Strategy remains a useful tool for Components to organize and monitor their data management plans. The key attributes and associated assessment questions include:

Attribute	Assessment Questions
Visible: Consumers can locate the needed data.	❑ Are authorized users able to discover the existence of data that is of particular interest or value? ❑ Are data stewards, data custodians, and functional data managers assigned responsibility for identifying, registering, and exposing data to make it easily discoverable across the enterprise, and to appropriate external partners? ❑ Are users able to discover and rapidly identify who is responsible for specific data products, the location of data products, the types of data products available, and the means of accessing the data products?
Accessible: Consumers can retrieve the data.	❑ Are authorized users able to obtain the data they need when they need it? ❑ Are data, including warfighting, intelligence, and business data, accessible to authorized users?
Understandable: Consumers can find descriptions of data to recognize the content, context, and applicability.	❑ Are tools in place that allow users to securely aggregate, compare, and analyze the data? ❑ Are the data labeled and formatted appropriately to support large scale analytics? ❑ Does the metadata associated with the data contain the contextual relationships and business rules?
Linked: Consumers can exploit complementary data elements through innate relationships.	❑ Are the data linked such that relationships and dependencies can be uncovered and maintained? ❑ Does the organization use industry best practices for open data standards, data catalogs, and metadata tagging? ❑ Are the data unnecessarily siloed or do they support connections across disparate sources?
Trustworthy: Consumers can be confident in all aspects of their use of the data for decision-making.	❑ Do the data represent a source of truth? ❑ Must the data undergo additional vetting to ensure it can support decision-making? ❑ Can users interpret and analyze data without concern for flawed assumptions, resulting in potentially fatal outcomes? ❑ Does the data reflect metadata or context necessary to enable consumers to make appropriate judgments about whether or how to rely on the data?

Attribute	Assessment Questions
Interoperable: Consumers and producers have a common representation and comprehension of data.	❑ Can the data be exchanged between systems and users while maintaining its quality and usability? ❑ Do the data have semantic as well as syntactic interoperability based on common data formats and machine-to-machine communications?
Secure: Consumers understand data safeguarding responsibilities, follow classification management procedures, and know that data is protected from unauthorized use and manipulation.	❑ Are the data protected while at rest, in motion, and in use (within applications, with analytics, etc.)? ❑ Does the organization use a disciplined approach to data protection, such as attribute-based access control, across the enterprise? ❑ Are protective mechanisms (e.g., security controls) in place for credentialed users to ensure that access is permitted in accordance with applicable laws, regulations, and policies? ❑ Are classified management procedures in place to ensure that data, aggregated or not, are safeguarded and in accordance with laws, regulations, and policies?

Taken together, these guidelines provide a foundation for organizations to greatly enhance the quality of high priority data sets in effective and efficient ways. Absent an organized approach based on tested criteria, Components will face significant challenges developing the level of data quality required to address analytics and artificial intelligence requirements. As such, organizations will use collaborative forums, such as the CDAO Council and its supporting forums, to flatten communications, enhance visibility, and ensure alignment across approaches to data quality improvement and maintenance.