SLIDES ONLY

NO SCRIPT PROVIDED

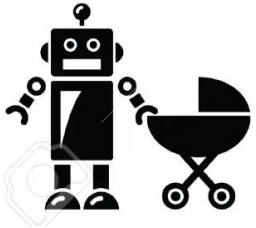
CDAO

AI/ML Scaffolding and AI Assurance

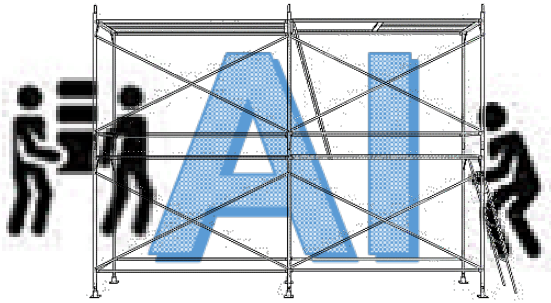
Dr. Bill Streilein

Key Takeaways - BLUF

- CDAO is developing AI scaffolding to support the adoption of AI across the DoD

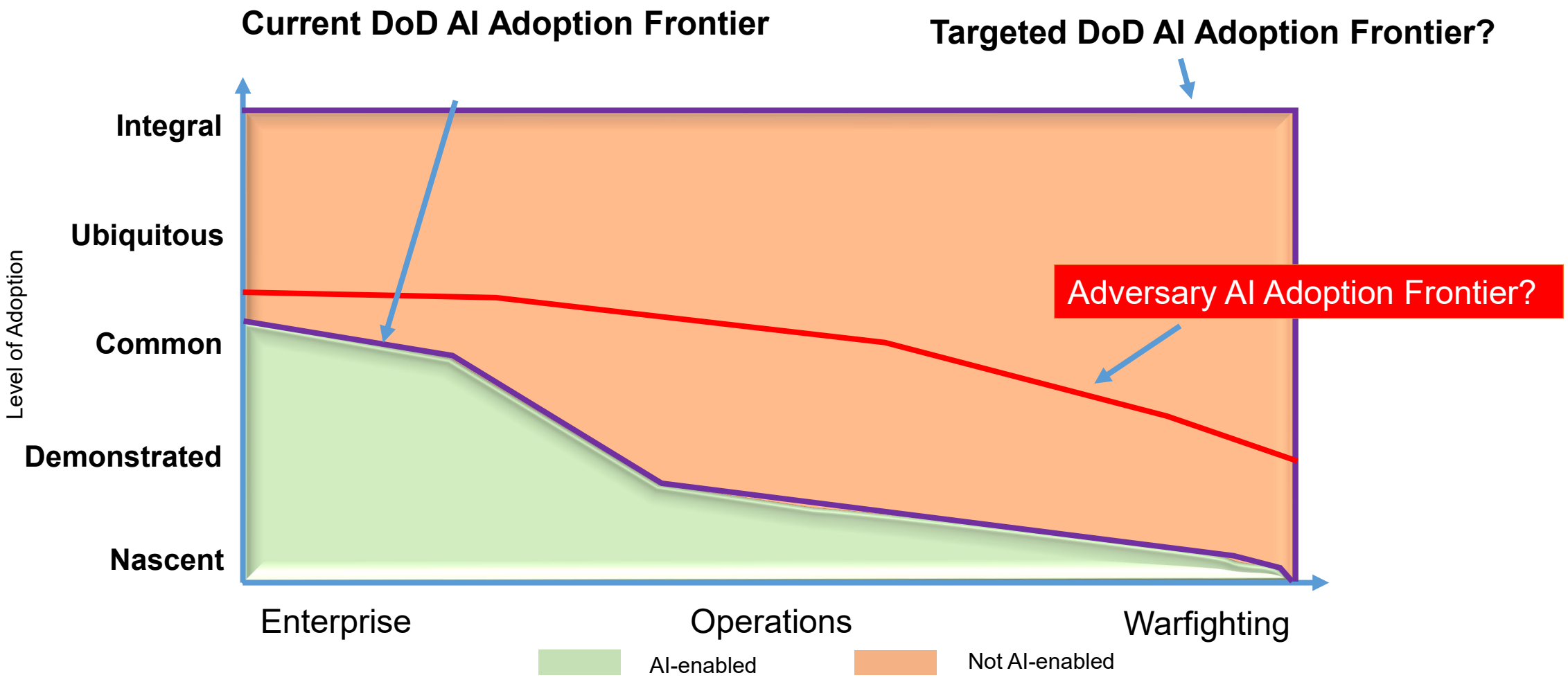


- Through scaffolding CDAO will provide, broker, and advise on the creation of platforms, apps, and services needed by DoD customers to enable the development and adoption of AI

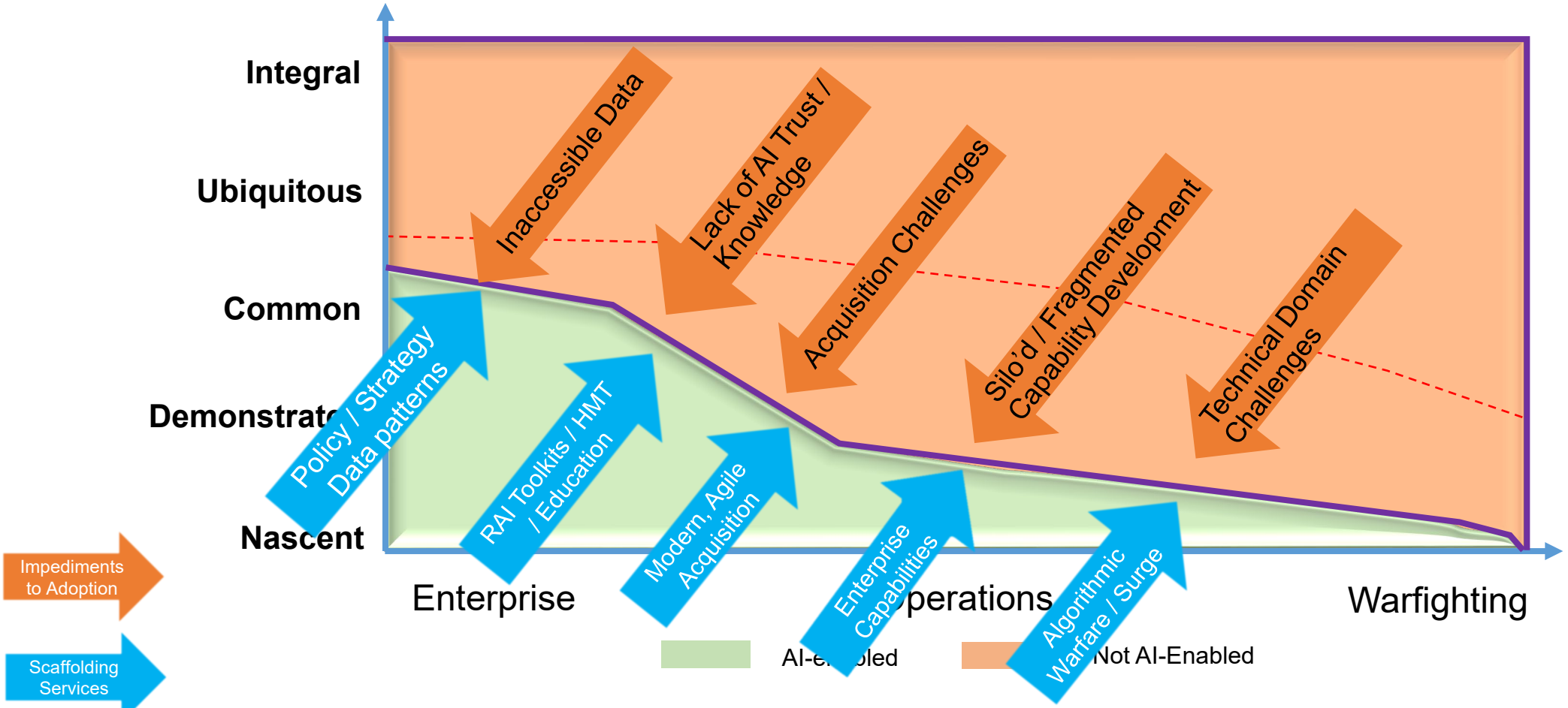


- **Desired Industry Day Outcome:** Industry partnerships in support of AI scaffolding

AI Adoption Framework



How Scaffolding Enables AI Adoption

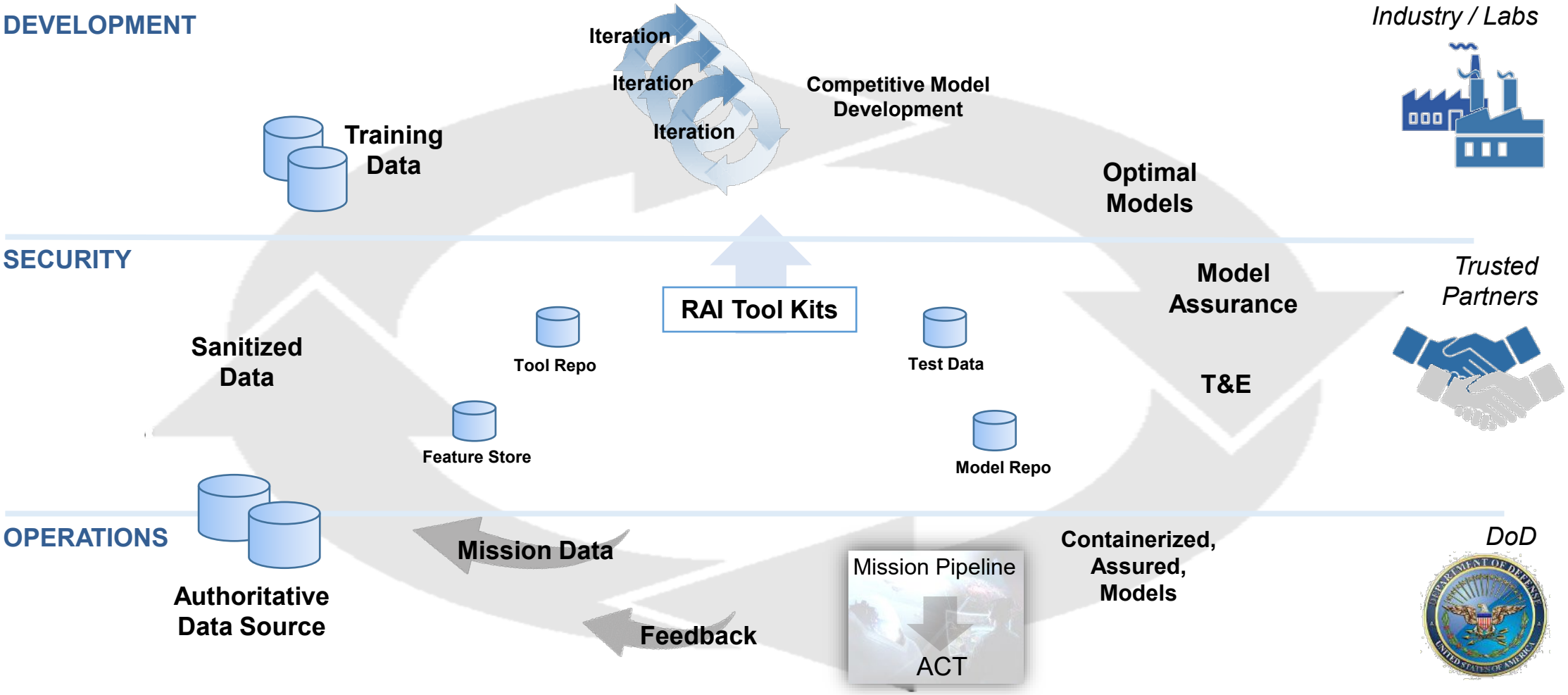


AI/ML Scaffolding will offer enabling services to address these challenges and accelerate adoption

Principles of AI/ML Scaffolding

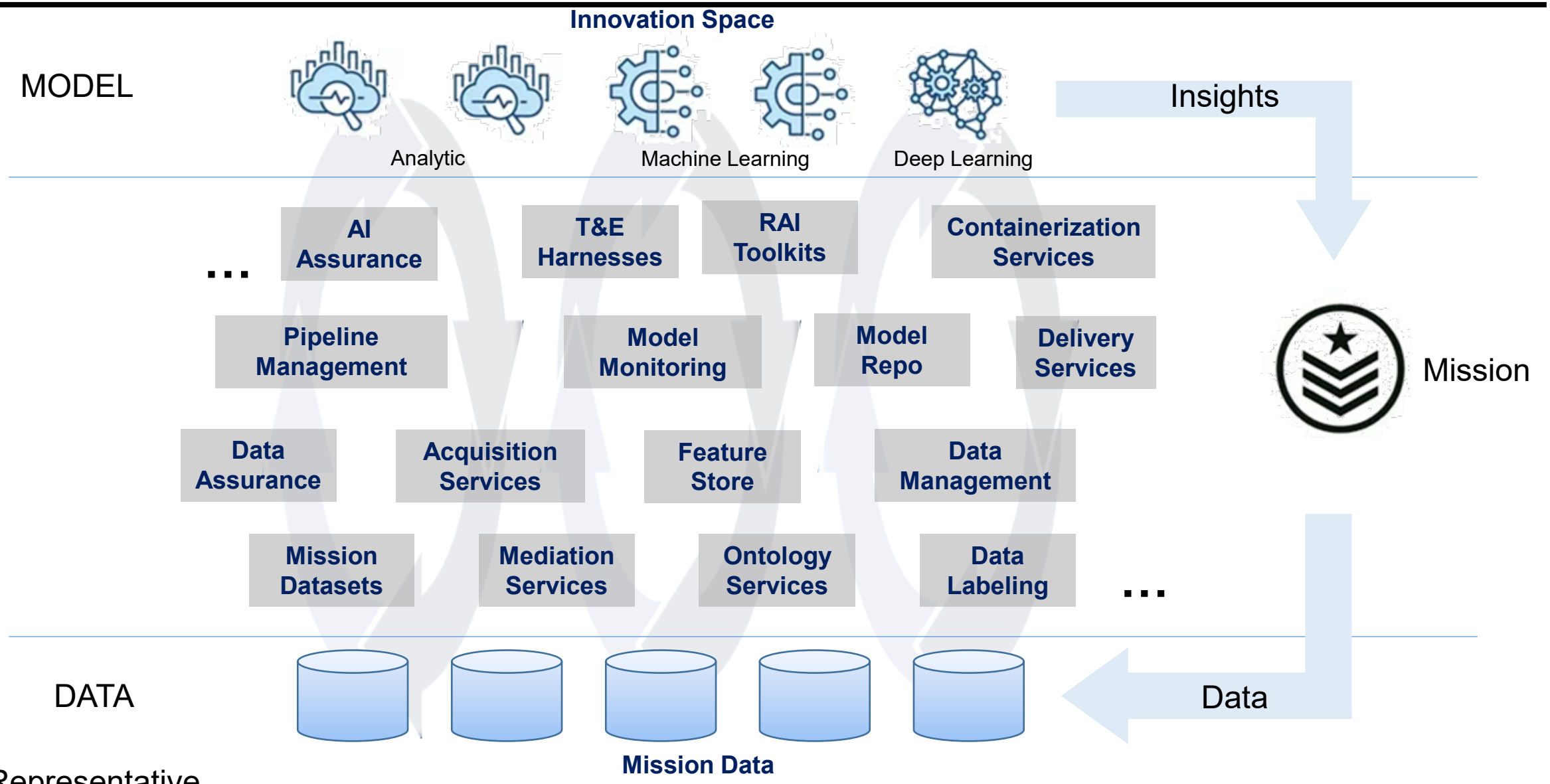
- ✓ **Enable DoD to leverage Assured AI to modernize mission functions**
- ✓ **Engender a Digital Ecosystem in which…**
  - ✓ **Industry innovation is enabled and leveraged,**
  - ✓ **Open architecture principles are used**
  - ✓ **DoD guidance, standards, and toolkits assure AI**
  - ✓ **Mission challenges are addressed**
- ✓ **Offer enterprise services to reduce barrier to entry, focus on mission**
- ✓ **Enable monitoring and management to drive enterprise goals**

AI/ML Scaffolding Digital Ecosystem



A distributed MLOPs loop brings assured innovation to meet mission need

AI/ML Scaffolding Services*



* - Representative

Potential Scaffolding Services

- Data services
  - Discoverability, transport, storage, conversion, labeling, ontologies, standards
- MLOPs services
  - Dev environments, federated model catalogs, pre-approved code & AI packages
- Instrumentation services
  - Model performance monitoring, user interactions
- AI Assurance services
  - T&E harnesses, methodologies, data partitioning
- Acquisitions services
  - Access to contract vehicles, contract language review
- Legal services
  - Data usage agreements, classification determinations
- AI Consulting

CDAO AI Assurance

AI Assurance Goal

Provide stakeholders with *justified confidence* that the DoD AI-enabled systems meet requirements and support mission through ethical action

Stakeholders include warfighter, commanders, PMs, acquisitions, regulators, tax payers, international allies

Arguments + Evidence = Justified Confidence

CDAO AI Assurance

Test and Evaluation

Responsible AI (RAI)

CDAO AI T&E Process

Integrity Testing
Test performance in normal situation

Confidence Assessment
Assess Calibration & Uncertainty Awareness

Robustness
Test performance on natural perturbation and transformation

Resilience
Perform adversarial testing

Areas of Interest

- Human Systems Integration (HIS)
- Sequential Test Design
- Learning Systems
- Explainable AI (XAI)
- Responsible AI (RAI)
- Adversarial / Red Teaming
- T&E in Deployment / Sustainment

DoD AI Ethical Principles

CDAO

Principle	Description
Responsible	DoD personnel will exercise **appropriate levels of judgment and care,** while remaining responsible for the development, deployment, and use of AI capabilities.
Equitable	The Department will take deliberate steps to **minimize unintended bias** in AI capabilities.
Traceable	The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with **transparent and auditable methodologies, data sources, and design procedure and documentation.**
Reliable	The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to **testing and assurance** within those defined uses across their entire life-cycles.
Governable	The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to **detect and avoid unintended consequences,** and the ability to **disengage or deactivate deployed systems** that demonstrate unintended behavior.

Examples of RAI Tools

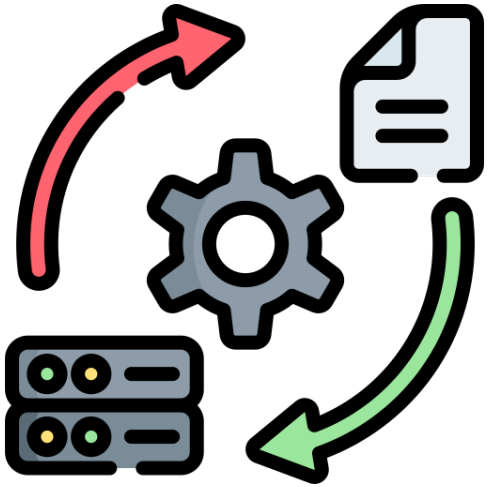
CDAO

RAI Tools function in a number of ways to support the operationalization of DoD's AI Ethical Principles for capability developers, RAI practitioners, and senior leaders.

What	Function	Example Tools
Technical or Software-Based	Helps developers and testers to assess factors such as bias, reliability, and safety	Data Bias Detection Tools Explainability Tools T&E Harness
Documentation and Artifacts	Provides traceability of data sources, model limitations, risk identification and mitigation efforts	Use Case/Harms Analysis Data Cards Model Cards
Frameworks and Checklists	Provides prompts to guide users in creating muscle memory around new processes for risk assessment and ethical considerations	Common Failure/Mishap List Algorithmic Impact Assessments Ethics Maturity Assessments User Research and Design Tools
Knowledge Sharing	Provides centralization for information sharing, learning, and common lexicon, practices, etc.	Use Case Repositories Information Management Systems
Executive Dashboards	Provides visibility into organizational compliance, status, and risk	Key Performance Metrics Progress Tracking

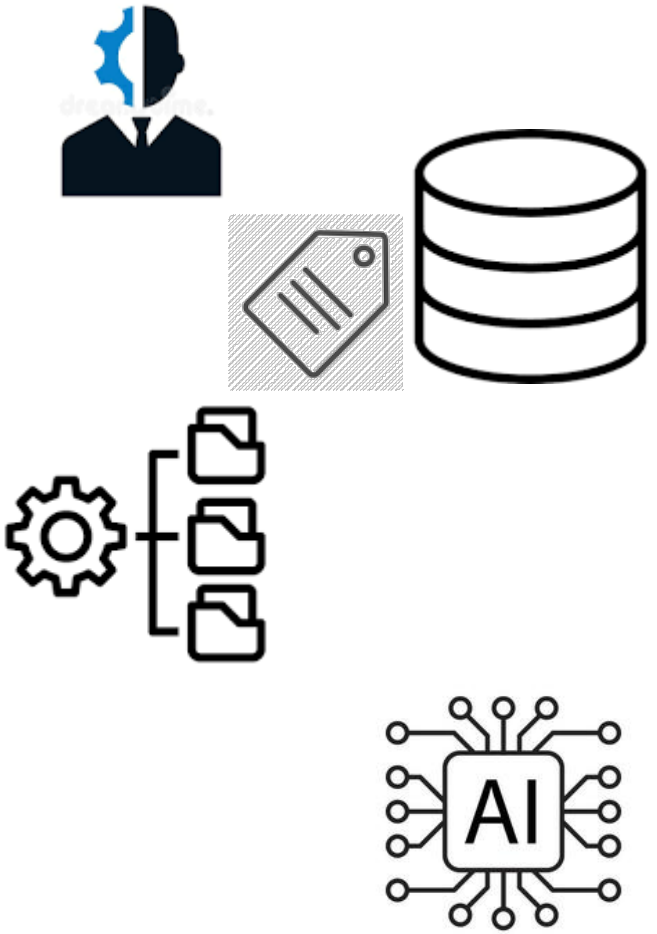
AI Consulting

- Project feasibility and requirements validation
  - Workflow mapping
- Adoption of standards
  - APIs, ABIs, data, formats, etc.
- Acquiring AI/ML development tools
- Selecting and implementing performance metrics
- UI/UX, User adoption, Utility to users
- Navigating DoD policy
  - RMF, software only assess
- Policy affecting AI/ML development and adoption



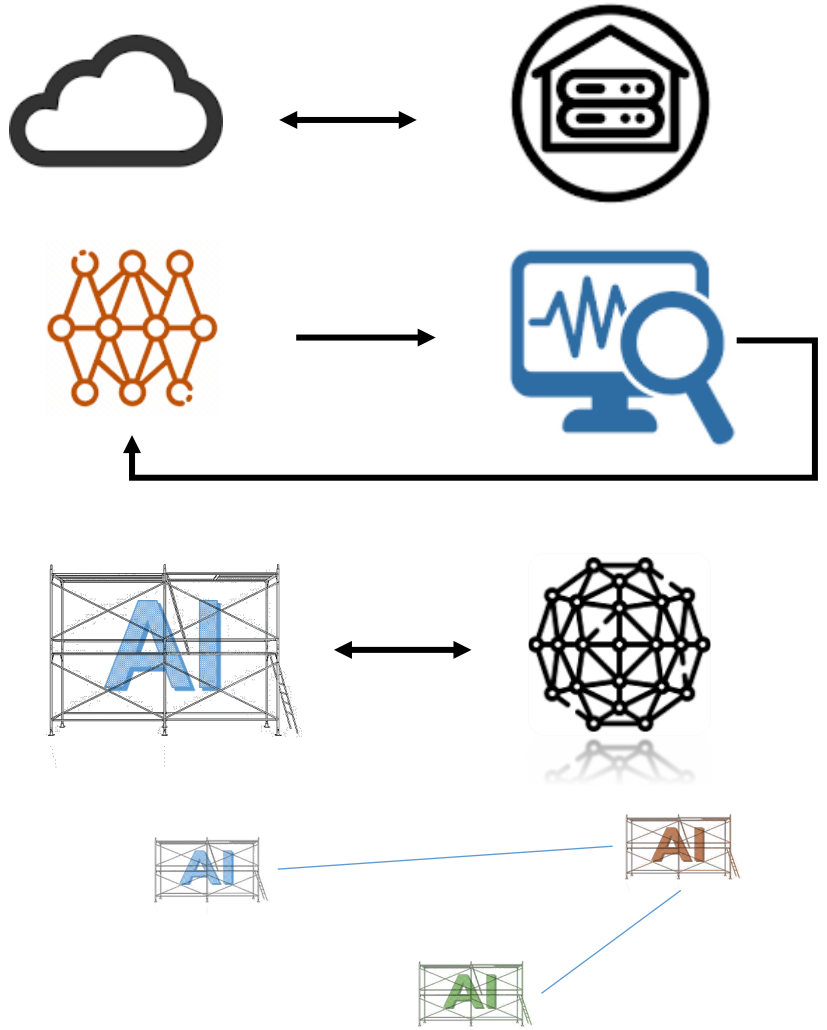
Immediate Industry Asks

- AI Consulting / Ideas on Scaffolding
- Data Labeling services
- AI Data Management Platform
- AI Assurance Capabilities
  - T&E / RAI



Relevant Tradespaces

- Cloud / On-Prem / Edge / Hybrid
- Role of feedback / model monitoring
- Interaction w/ the Data Mesh
- Scaffolding Federation



Next Steps

- White papers on relevant capabilities

- Technology demonstrations for scaffolding, etc.
  - Operationally-relevant use cases
  - Comparison w/ state of the art
  - Technical maturity
  - Scalability
  - Interoperability

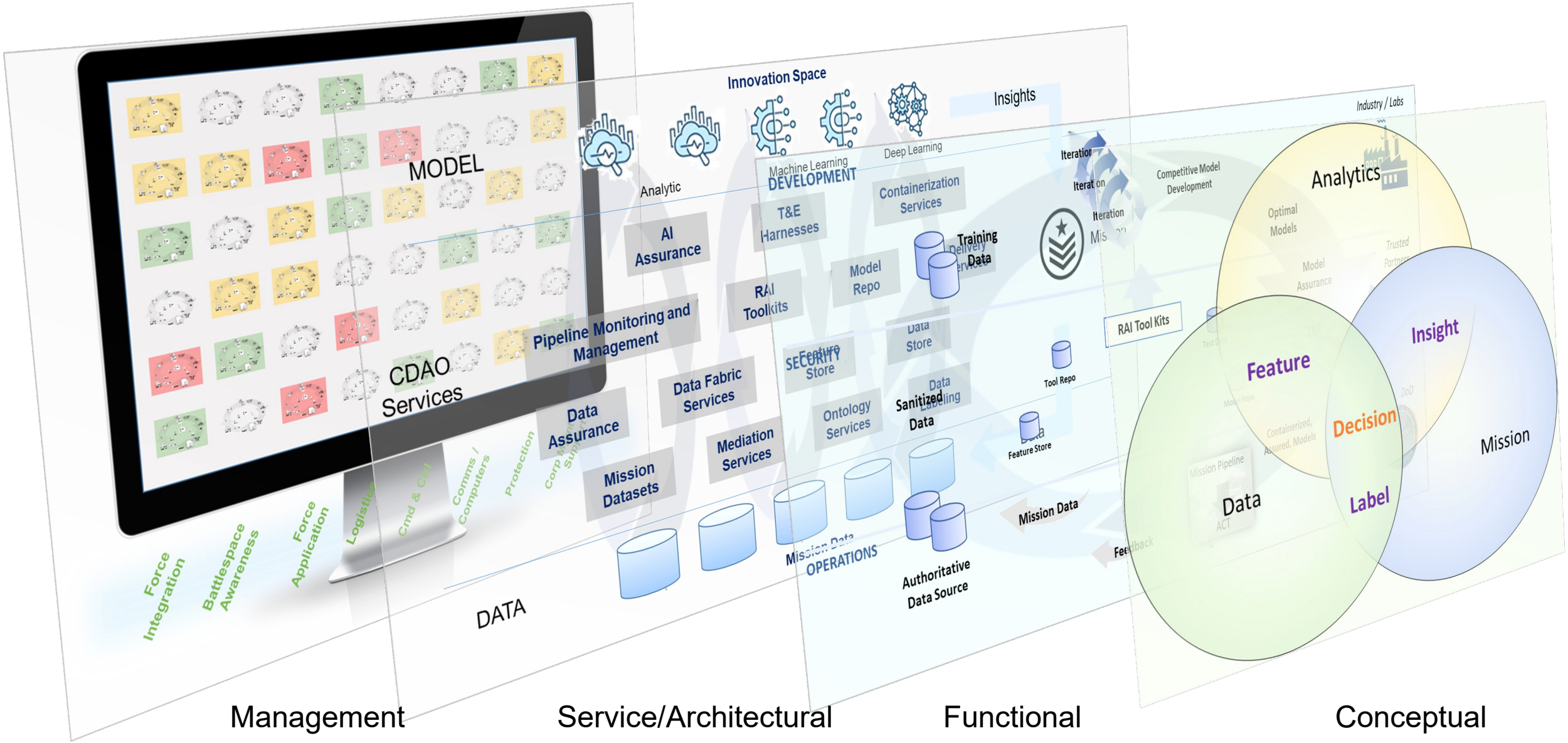
- Cost model for doing business

POCs

- Mr. Joe Larson – Deputy CDAO for Algorithm Warfare
  - joseph.p.larson.civ@mail.mil
- COL Tom Kilbride – Principal Director Algorithmic Warfare
  - thomas.j.kilbride.mil@mail.mil
- CAPT Xavier Lugo – AI/ML Scaffolding Lead
  - manuel.x.lugo.mil@mail.mil
- Dr. William Streilein – Chief Technology Officer
  - william.w.streilein.civ@mail.mil

Backup

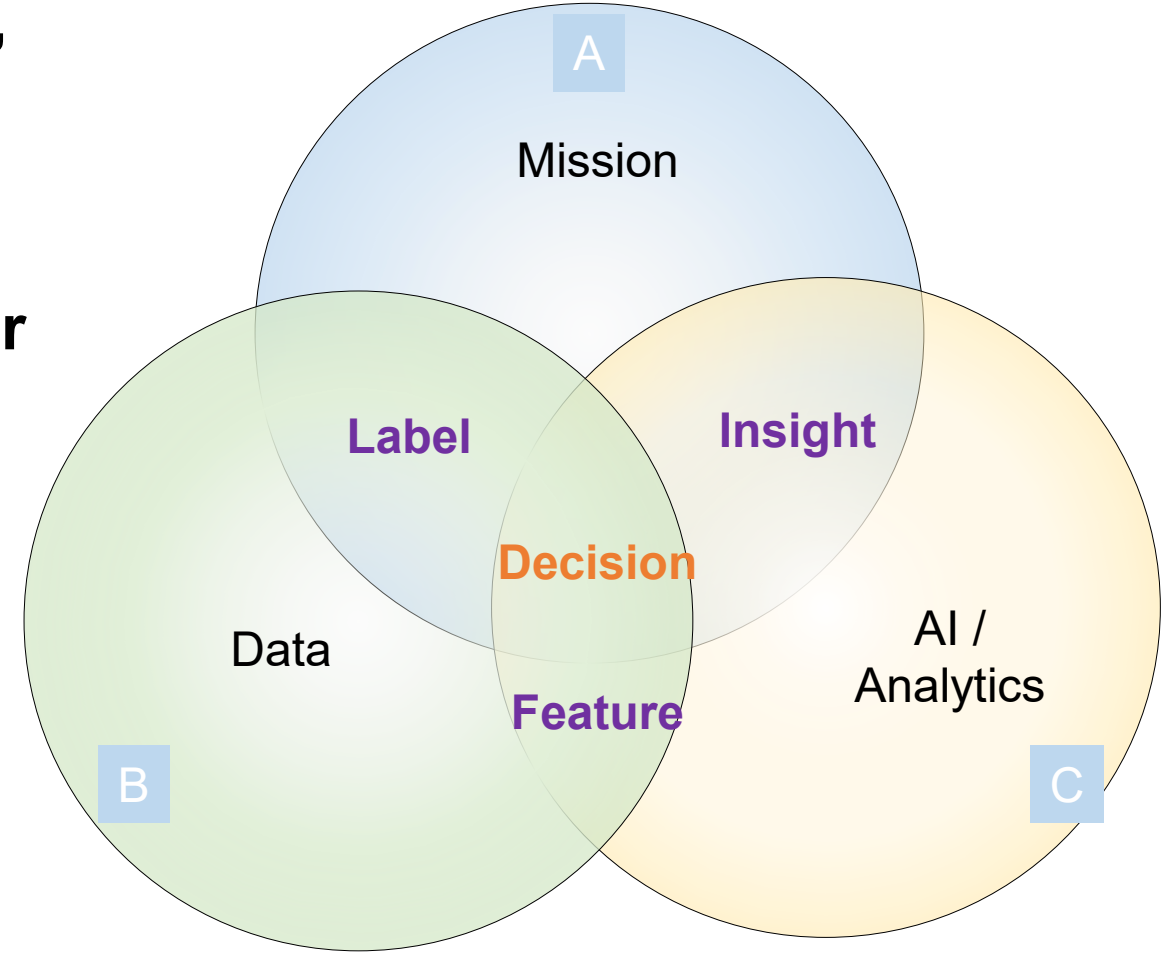
AI/ML Scaffolding Vision



Conceptual Layer

Depicts relationship between mission, data and AI/analytics to enable decision advantage.

- ✓ **Identify mission relevant *decision* or challenge**
- ✓ **Collect and label relevant *data***
- ✓ **Create *features* that support AI and analytics**
- ✓ **Operate on features to provide *insights* to mission**



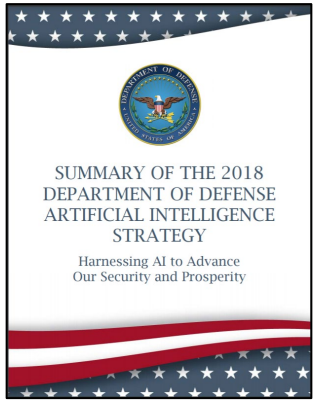
RAI Implementation Tenets

CDAO

Tenet	Description
RAI Governance	Ensure disciplined **governance structure and processes** at the Component and DoD-wide levels for oversight and accountability and clearly articulate DoD guidelines and policies on RAI and associated incentives to accelerate adoption of RAI within the DoD.
Warfighter Trust	Ensure warfighter trust by providing education and training, establishing a **test and evaluation and verification and validation (TE/VV) framework** that integrates real-time monitoring, algorithm confidence metrics, and user feedback to ensure trusted and trustworthy AI capabilities.
AI Product and Acquisition Lifecycle	Develop **tools, policies, processes, systems, and guidance** to synchronize enterprise RAI implementation for the AI product throughout the acquisition lifecycle through a systems engineering and risk management approach.
Requirements Validation	Incorporate RAI into all applicable AI requirements, including **joint performance requirements** established and approved by the Joint Requirements Oversight Council, to ensure RAI inclusion in appropriate DoD AI capabilities.
Responsible AI Ecosystem	Build a robust national and global RAI ecosystem to improve intergovernmental, academic, industry, and stakeholder collaboration, including cooperation with allies and coalition partners, and to **advance global norms grounded in shared values**.
AI Workforce	**Build, train, equip, and retain** an RAI-ready workforce to ensure robust talent planning, recruitment, and capacity-building measures, including workforce education and training on RAI.

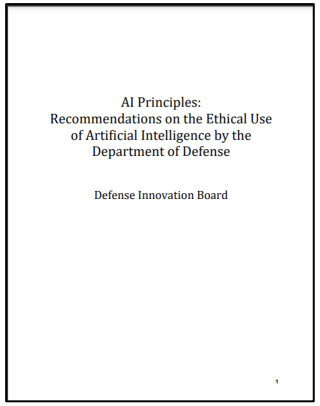
AI Policy and Strategy Evolution

Guidance Documents



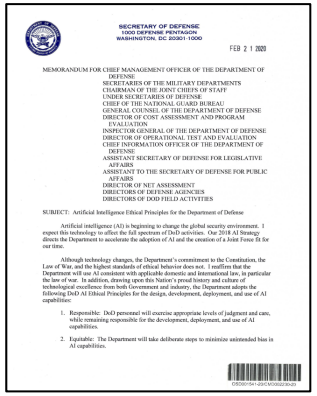
June 2018: DoD AI Strategy

The Department released an unclassified summary of the 2018 DoD AI Strategy, which identified one of its five pillars as "leading in military ethics and AI safety" and pledged to articulate its vision and guiding principles for using AI in a lawful and ethical manner.



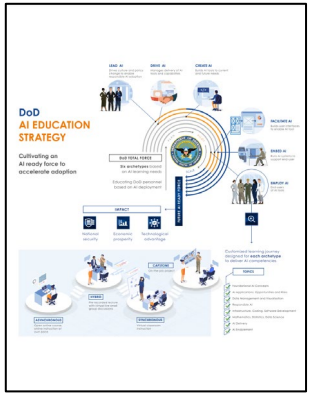
October 2019: DIB Report

The Defense Innovation Board (DIB) proposes AI Ethics Principles for DoD for the design, development, deployment, and use of AI for both combat and non-combat purposes.



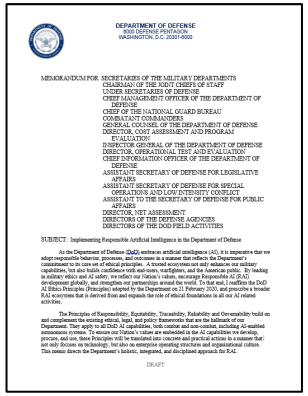
February 2020: AI Ethical Principles Memo

The DoD formally adopts five AI ethical principles and designates the JAIC as DoD's lead for coordination and implementation of the Principles.



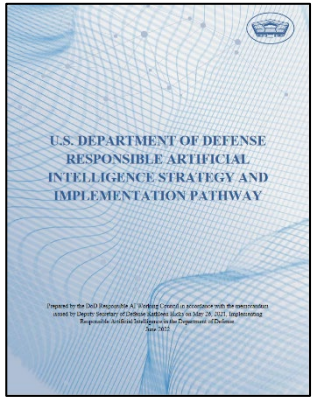
October 2020: DoD AI Education Strategy

The Department establishes an overarching strategy to cultivate an AI-ready force to accelerate the adoption of AI.



May 2021: Implementing RAI in the DoD Memo

The Deputy Secretary of Defense reaffirms the DoD AI Ethical Principles and directs the JAIC to coordinate actions to accelerate the adoption and implementation of Responsible AI.

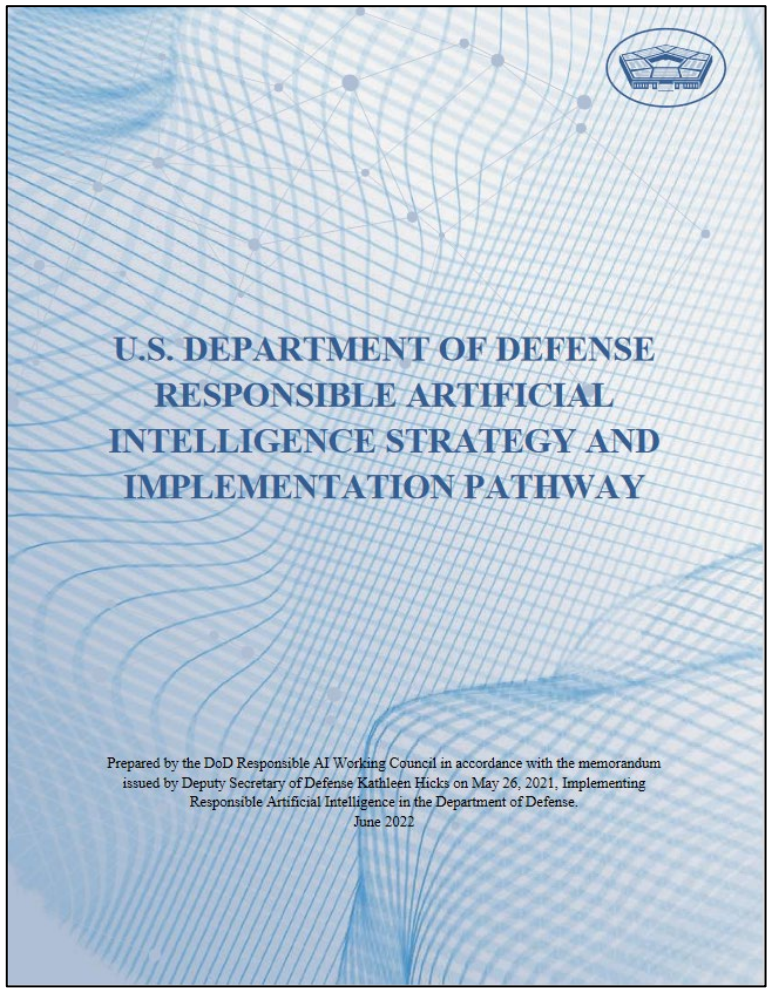


June 2022: RAI Strategy and Implementation Pathway

The Department outlines the strategic approach for operationalizing the DoD Ethical Principles while ensuring operational agility, scalability, and speed of deployment.

RAI Strategy & Implementation Pathway

CDAO



June 2022

Outlines the Department's Strategy for Operationalizing the Ethical Principles

Within this document, the Deputy Secretary of Defense:

- Explains the Department's approach to Responsible AI
- Establishes over 60 lines of effort aligned with the RAI implementation tenets
- Defines governance, roles, and responsibilities within the Department

Highlights

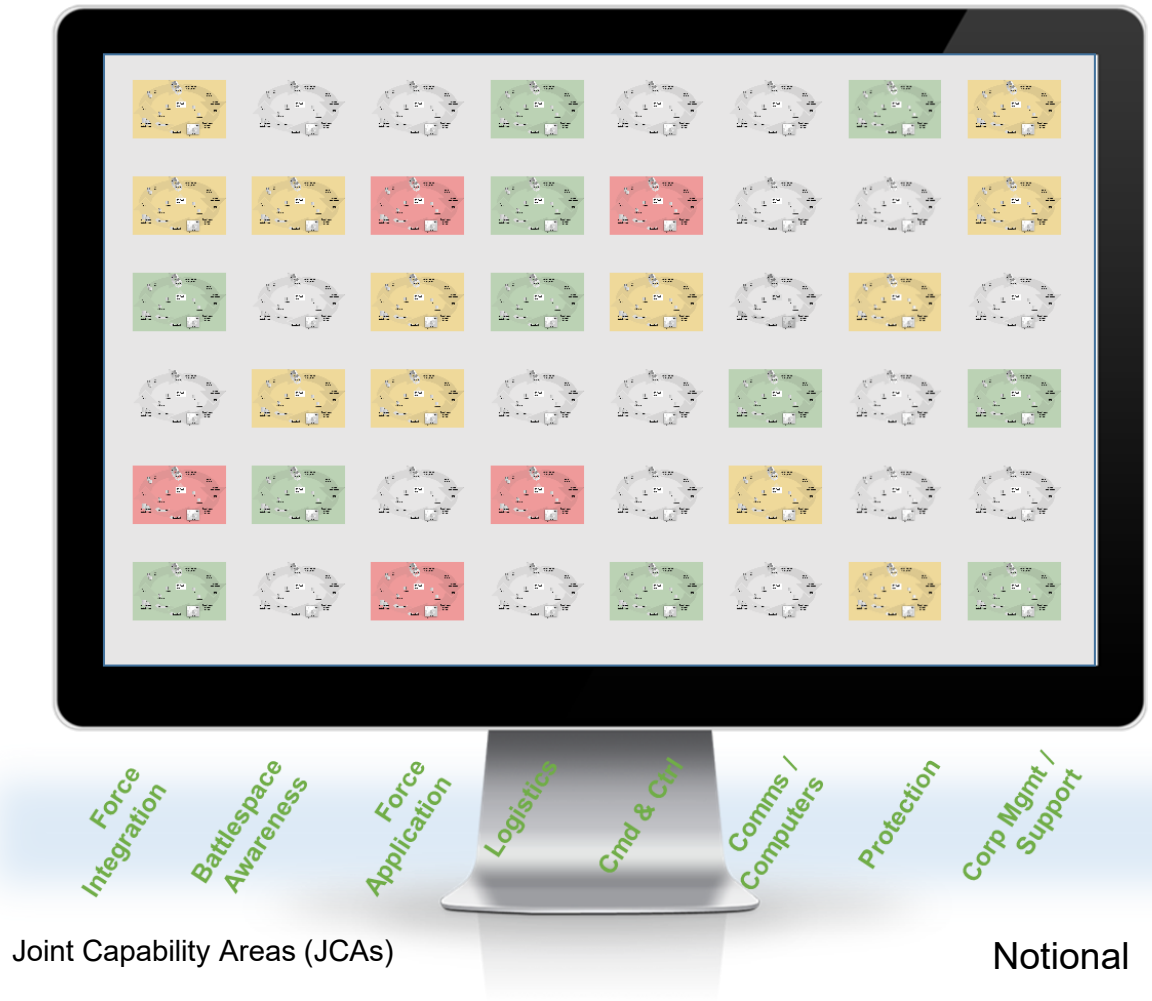
- Continued focus on warfighter trust as desired end state
- Desire to preserve speed, agility, and efficiency

Monitoring / Management Layer

CDAO

Track status of adoption across DoD enterprise

- ✓ ***Instrument*** **the distributed MLOPs pipeline at each step**
- ✓ ***Aggregate*** **status across joint mission areas**
- ✓ **Leverage insights to *direct* investment towards adoption goals**



Notional