INSTITUTE FOR DEFENSE ANALYSES

# DATAWorks 2024: Data Verification, Validation, and Accreditation for AI-Enabled Capabilities


Rachel Haga, Project Leader

John W. Dennis
Erin P. Eifert
David M. Tate
Connor P. Trask



March 2024





IDA Product 3001831

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, BM-9-5153, for the Office of the Chief Digital and Artificial Intelligence Officer.
The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Dr. V. Bram Lillard and consisted of Dr. Heather Wojton, Dr. John Haman, Dr. Miriam Armstrong, Dr. Steven Movit, Dr. Kelly Tran, Dr. Keyla Pagan-Rivera, and Dr. Rebecca Medlin from the Operational Evaluation Division.

For more information:
Dr. Rachel Haga, Project Leader
rhaga@ida.org• 703-578-2768

Dr. V. Bram Lillard, Director, Operational Evaluation Division
vlillard@ida.org • (703) 845-2230



Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Product 3001831

# DATAWorks 2024: Data Verification, Validation, and Accreditation for AI-Enabled Capabilities

Rachel Haga, Project Leader

John W. Dennis
Erin P. Eifert
David M. Tate
Connor P. Trask

# Executive Summary

Data is a crucial component for the development and support of artificial intelligence (AI)-enabled systems, making the data lifecycle, including collection, preparation, and curation, an important part of the AI lifecycle. Ensuring that the data are consistent, correct, and representative for their intended use is critical to ensuring the efficacy of an AI-enabled system. Data verification, validation, and accreditation (VV&A) is meant to address this need. The dramatic increase in the prevalence of AI-enabled capabilities and analytic tools across the DoD has emphasized the need for a unified understanding of data VV&A, as quality data forms the foundation of AI models. In practice, data VV&A and associated activities are often used in an ad-hoc manner that may limit the ability to support development and testing of AI-enabled capabilities. However, existing DoD frameworks and policy for data VV&A are applicable to the AI lifecycle and embody important supporting activities for test and evaluation of AI-enabled systems. We highlight the importance of data VV&A and discuss the applicability of DODI 5000.61 to AI models and their associated data. Relying solely on definitions from policy leaves questions regarding interpretation and implementation, so we discuss some potential concerns and best practices, including consideration of data VV&A in the context of the lifecycle of the AI-enabled system, encouraging reproducibility and transparency, and supporting VV&A with existing frameworks and tools.

# DATAWorks 2024: Data VV&A

## for AI-Enabled Capabilities

*John W. Dennis, Erin Eifert, David Tate, Connor Trask*

*April 2024*

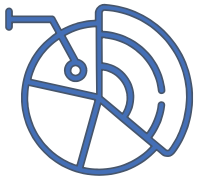
**Sponsored By**

Chief Digital & Artificial Intelligence Office
Assessment & Assurance

# What is Data VV&A?

The process of verifying the internal consistency and correctness of data and validating that it represents real-world entities appropriate for its intended purpose or an expected range of purposes.

- DoDI 5000.61



**Verification**
Satisfies specifications and requirements

**Validation**
Appropriately represents the real world

**Accreditation**
Determines acceptability for a specific use



IDA | CDAO

# What is Data VV&A?

- **Verification**: Do the data satisfy the developer's conceptual description, specifications, and requirements?

- **Validation**: Do the data accurately represent the real world with respect to the intended use of the model?
  - *Not to be confused with a validation set (used for hyperparameter tuning)!*

- **Accreditation**: Are the data acceptable for use for a specific purpose?
  - V&V'd for a specific use
  - The neighborhood of use cases where V&V conveys
  - A data set and its lifecycle may be accredited for multiple uses. V&V for different uses will likely overlap!



IDA | CDAO

# Why do we need Data VV&A for AI?

Lots of emphasis on the AI **Model**

- As the primary thing of interest (T&E)
- or as supporting the thing of interest (V&V)
- Easy to overlook V&V of the data

Data Work Modeling

Data are the foundation of AI models

- Data quality matters (Garbage in ⇒ Garbage out)
- Data work can easily be the largest component of the AI pipeline
- The use case matters for the data, not just the model!
- Having a list of accredited use cases can facilitate curation, access, development, and testing

**V&V of Data is also mandated by policy!**



IDA | CDAO

# DOD recognizes the need to VV&A data

DoDI 5000.61

- **Purpose**: Establishes policy, assigns responsibilities, and prescribes procedures for the VV&A of models, simulations, distributed simulations, **and their associated data**.

- **Applicability**: Models and simulations and associated data developed, used, made available, or managed by the DoD Components, to include those used by non-DoD organizations to support DoD processes, products, or procedures.

- **Policy:**
  - Models, simulations, **and associated data** **used to support DoD processes, products, and decisions** **shall undergo verification and validation (V&V)** throughout their lifecycles.
  - Models, simulations, and associated data used to support DoD processes, products, and decisions **shall be accredited for an intended use**.



IDA | CDAO

# Applicability to AI-Enabled Capabilities

DoDI 5000.61

DoDI 5000.61 is broad.

- **Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process**
  - Examples include a mathematical formula, etc.

- Policy scope: **used to support DoD processes, products, and decisions**

Context for the model may be different
- Support vs. system under test

Applicability indicated beyond scope of traditional M&S,
- e.g. any model and any data owned, used, managed, etc. by DoD

How to VV&A is not covered
- Some of the “how” is different for data associated with AIEC

Data is not defined



IDA | CDAO

# What is Data VV&A?

Examples

**Verification:**

Are these data suitable for training/testing an ML model?

Correct

Consistent

Appropriately formatted

Normalized

Timely, Current

Adequate number

Absence of data poisoning

Absence of unwanted bias

Provenance

Accessible

**Validation:**

Are these data mission-appropriate for this system?

Complete/Full coverage of mission space

Representative with respect to labels/events

Include all important features

Secure

Anonymized

Corroborated

**Accreditation:**

For what range of missions could this dataset be used?

Environments

Mission goals

Human-machine concepts of employment

Consequences for non-accredited uses?

Additional V&V for a new proposed mission context?

What breaks accreditation?



IDA | CDAO

# Considerations for VV&A of Data

- **What do we consider "the data"?**
- **What are the requirements?**
  - What does it mean for the data to meet requirements?
- **What are the intended use cases?**
  - What does it mean to support the intended use case?
- **How do you define and measure operational realism?**
- **What defines "acceptable"?**

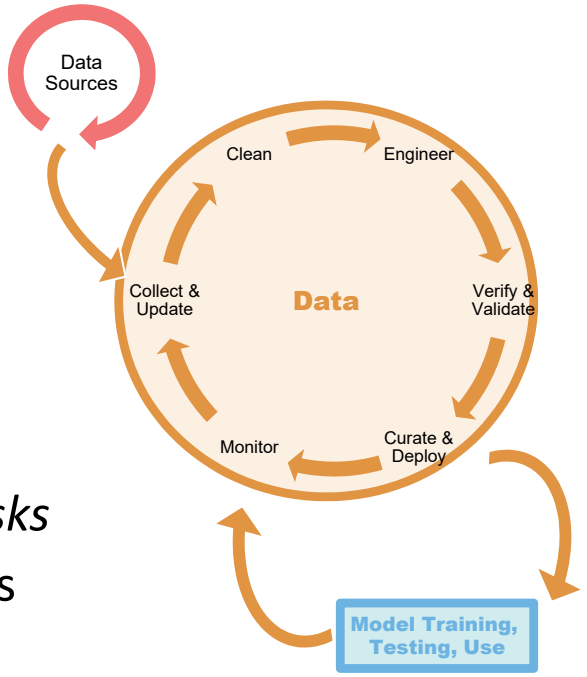
# Considerations for VV&A of Data

What is “the data”?

**AI models are developed and tested iteratively**

- ***Lifecycle considerations*** – cleaning, engineering, preparation
  - Data is often processed before being passed to the model

- ***Meta-data***
  - *Helps us understand correctness, applicability, and risks*
  - Calculations, process info, judgment, and descriptions
  - Provenance
  - Data card – ensure it is complete, correct, and up to date!




IDA | CDAO

# Considerations for VV&A of Data

What are the requirements?

- **Lifecycle Considerations**
  - May include mandates for cleaning, producing metrics, and timeliness
  - Boundaries matter (e.g. contractors, data providers)
  - Design choices may change over the lifecycle

- What kinds of bias are you okay with and what are you not?
  - What if those elements are driven by latent information? What info does V&V require?
- Privacy and security?  Ethical Sourcing?
- Coverage/Completeness, & Correctness
  - Are there acceptable levels of misses?
- Size limits, cadence (e.g., this needs to be done or updated monthly).

# Considerations for VV&A of Data

Intended use cases?

Use in a particular model/system/environment with a specific goal.

- What is the learning paradigm? Are the data appropriate?
- What is the operational environment? Are the data representative?
- What are the interfaces?
  - People? Other systems? Do the data capture the right information?
- Are the labels aligned with and appropriate for the intended use? (relabeling/revising a data ontology can be expensive!)
- What kinds of bias matter?

# Considerations for VV&A of Data

## Operational Realism?

- How do you define and measure operational realism?
  - How do you define mission success?
  - Can the data be used to measure operational realism?
  - Can the data be used to measure mission success?

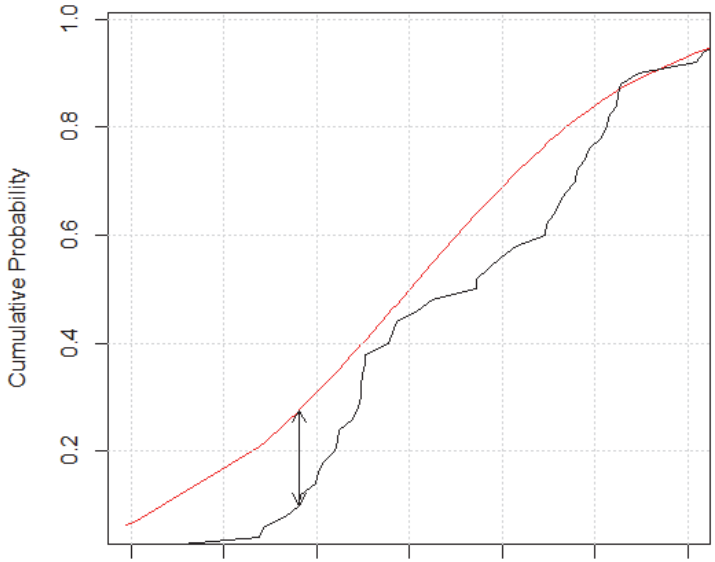
- What level of fidelity is appropriate/sufficient?
  - Granularity and coverage?
  - Spurious relationships?
  - May induce incorrect or undesirable results in AIES.

# Considerations for VV&A of Data

Acceptability criteria?

How do you know if the data is good enough?

- When to use quantitative vs. qualitative measures?
- When is measurement difficult?




What triggers a need to update or redo V&V?

- What breaks accreditation?
- For example, does data drift imply the need to reaccredit?



IDA | CDAO

# How do we VV&A data?

Minimum documentation requirements (stated)

- Date and POC/authority
- Version/release
- Intended use(s)
- List of requirements
- List of **assessment activities**
- Summary of results
  - including limitations, risks, potential impacts, and assumptions
- Accreditation criteria

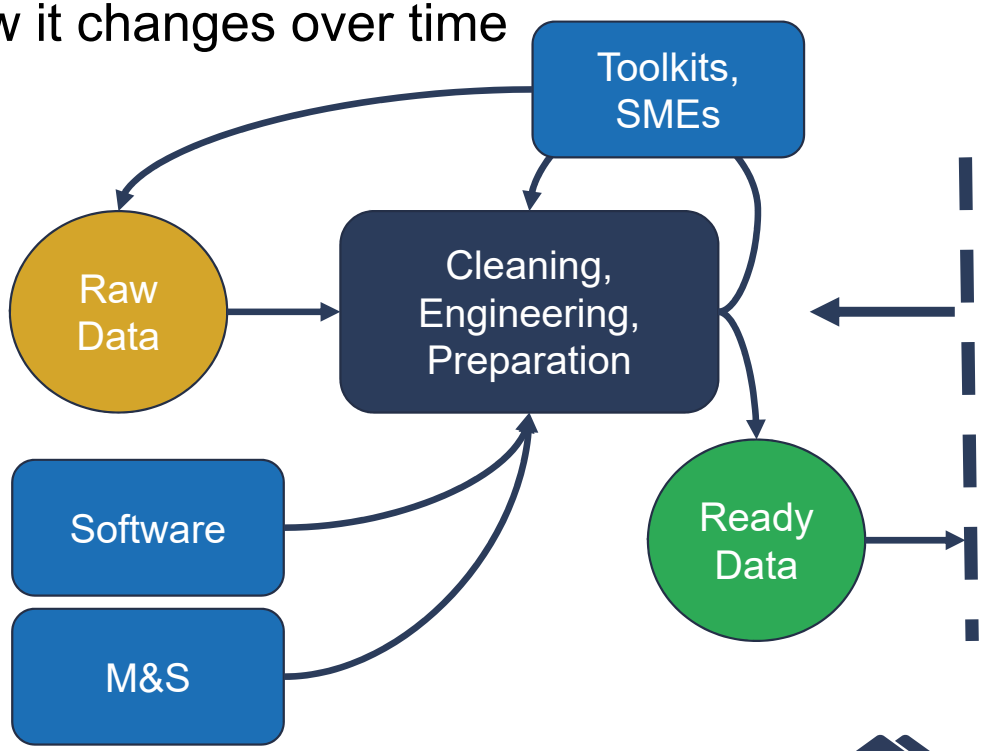



IDA | CDAO

# How do we VV&A data?

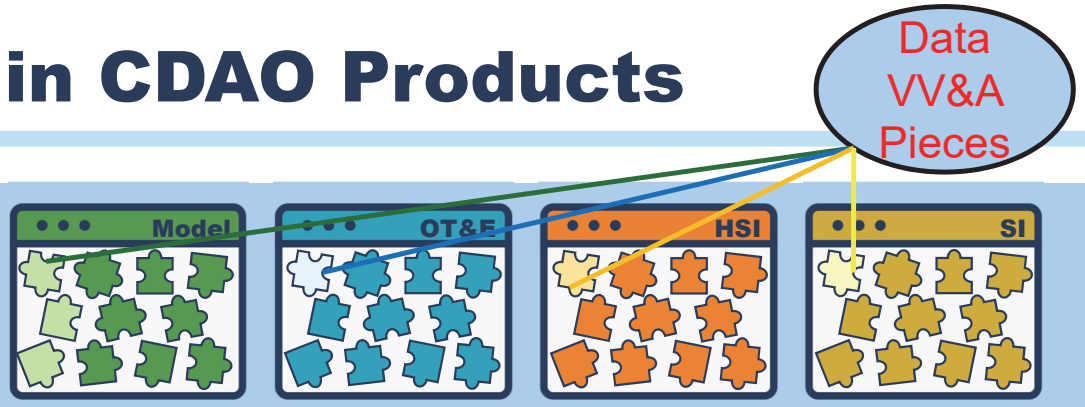
Best Practices

- Consider data VV&A in the context of the AI system lifecycle
  - Think about the context and how it changes over time
- Do by code
- Document & version everything
- Support with known frameworks
  - Software TEV&V
  - M&S V&V
- And existing tools
  - RAI Toolkit
  - JATIC Toolkit




IDA | CDAO

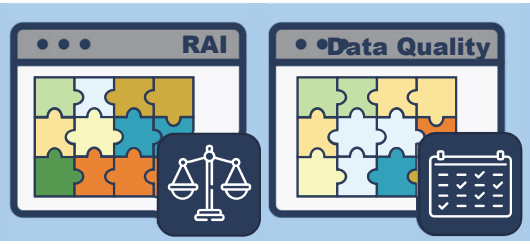
# Data VV&A in CDAO Products




**Test & Evaluation Strategy Frameworks**

**(Forthcoming)**

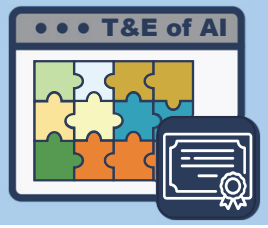
Foundational understanding for AI and/or DoD T&E novices




**Use Case Guidebooks + Codebooks**

**(In Progress)**

Concrete, tailored guidance mapped to a particular use case




**Workforce Training**

**(In Progress)**

Workforce training credentials, courses and materials



IDA | CDAO

jdennis@ida.org

# Back up slides

# What is VV&A?

## 5000.61 literal definitions

- **Verification:** The process of determining that a model or simulation implementation and its associated data accurately represent the developer's conceptual description and specifications.

- **Validation:** The process of determining the degree to which a model or simulation and its associated data are an accurate representation of the real world from the perspective of the intended uses of the model.

- **Accreditation:** The official certification that a model or simulation and its associated data are acceptable for use for a specific purpose.

# Text to Image Generation


MS Copilot (DALL-E 3)


Adobe Illustrator

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| XX-04-2024 | Final | |

**4. TITLE AND SUBTITLE**

DATAWorks 2024: Data Verification, Validation, and Accreditation for AI Enabled Capabilities

**5a. CONTRACT NUMBER**

HQ0034-19-D-0001

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

John W Dennis, III
Erin P Eifert
David M Tate
Connor P Trask

**5d. PROJECT NUMBER**

BM-9-5153

**5e. TASK NUMBER**

5153

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Institute for Defense Analyses
730 East Glebe Road
Alexandria, Virginia 22305

**8. PERFORMING ORGANIZATION REPORT NUMBER**

3001831

3001831

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Office of the Chief Digital and Artificial Intelligence Officer

**10. SPONSOR/MONITOR'S ACRONYM(S)**

CDAO

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Distribution Statement A. Approved for public release: distribution is unlimited.

**13. SUPPLEMENTARY NOTES**

Project Leader: Rachel A Haga

**14. ABSTRACT**

Data – collection, preparation, and curation - is a crucial need in the AI lifecycle. Ensuring that the data are consistent, correct, and representative for the intended use is critical to ensuring the efficacy of an AI enabled system. Data verification, validation, and accreditation (VV&A) is meant to address this need. The dramatic increase in the prevalence of AI-enabled capabilities and analytic tools across the DoD has emphasized the need for a unified understanding of data VV&A, as quality data forms the foundation of AI models. In practice, data VV&A and associated activities are often used in an ad-hoc manner that may limit the ability to support development and testing of AI enabled capabilities. However, existing DOD frameworks for data VV&A are applicable to the AI lifecycle and embody important supporting activities for T&E of AI enabled systems. We highlight the importance of data VV&A, relying on established definitions, and outline some concerns and best practices.

**15. SUBJECT TERMS**

data, verification, validation, V&V, VV&A, artificial intelligence, AI

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Rachel A Haga |
| Unclassified | Unclassified | Unclassified | SAR | 24 | 19b. TELEPHONE NUMBER *(Include area code)* 703-578-2768 |