BY ORDER OF THE COMMANDER SPACE TRAINING AND READINESS COMMAND

SPACE TRAINING AND READINESS COMMAND INSTRUCTION 90-7002

28 MAY 2026

Special Management

MODEL MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ STARCOM/CDAO

Certified by: HQ STARCOM/CDAO

Pages:

This instruction implements Air Force Policy Directive (AFPD) 90-70, *Enterprise Data Management*, and is consistent with Department of Defense Instruction (DoDI) 5000.61, *DoD Modeling and Simulation Verification, Validation, and Accreditation*; DoDI 5000.70, *Management of DoD Modeling and Simulation (M&S) Activities*; DoDI 5000.82, *Requirements for the Acquisition of Digital Capabilities*; DoDI 5000.88, *Engineering of Defense Systems*; DoDI 5000.97, *Digital Engineering*; DoD Manual (DoDM) 5000.102, *Modeling and Simulation Verification, Validation, and Accreditation for Operational Test and Evaluation and Live Fire Test and Evaluation*; DoDI Instruction 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense;* Department of Defense Directive (DoDD) 3100.10, *Space Policy*; Military Standard (MIL-STD) 3022, *Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations*; Air Force Instruction (AFI) 16-1001, *Verification, Validation and Accreditation (VV&A)*; Space Force Instruction (SPFI) 16-1002, *Threat Modeling, Simulation, and Analysis Guidance*; STARCOM Instruction (STARCOMI) 90-700, *Data Management*. This instruction applies to STARCOM individuals at all levels who develop, manage, review, disseminate or use United States Space Force (USSF) models, including all civilian employees and uniformed members of STARCOM and those with a binding agreement or contractual obligation to abide by the terms of STARCOM issuances. This instruction does not apply to the Air National Guard, Air Force Reserve Command, or the United States Air Force. This STARCOMI identifies Model Management guidelines for leveraging models as strategic and operational assets to meet USSF mission requirements. It also establishes the STARCOM guidance to achieve Field Command (FLDCOM)-wide models, visibility and accessibility, and addresses standards for model development and sharing under the direction of

the Chief Data and Artificial Intelligence Officer (STARCOM/CDAO). This instruction may be supplemented at any level, but all supplements that directly implement this instruction must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. This Instruction specifies how to maintain information protected by the Privacy Act of 1974 authorized by DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the OPR using Department of the Air Force (DAF) Form 847, *Recommendation for Change of Product*; route DAF Forms 847 from the field through the appropriate functional chain of command. Submit requests for waivers through the chain of command to the publication OPR for non-tiered compliance items.

Chapter 1—MODEL MANAGEMENT **4**

1.1. Background. 4

1.2. Model Management (MM). 4

Chapter 2—MODEL TYPES **5**

2.1. Model Types. 5

2.2. Digital Models (DM) Per DoD Instruction 5000.97: 5

2.3. DT/AI Models. 6

Chapter 3—MODEL STANDARDS **8**

3.1. Model Standards. 8

3.2. Taxonomy. 8

3.3. Standards Compliance. 8

3.4. MOSA and Open Interfaces. 8

3.5. Interoperability Verification. 8

3.6. Standardized Model Interface (SMI). 8

Chapter 4—MODEL CATALOGING, METADATA, AND STORAGE **9**

4.1. Cataloging. 9

4.2. Metadata Tagging. 9

4.3. Model Storage. 11

Chapter 5—MODEL SHARING **12**

5.1. Intra-Service Model Sharing. 12

5.2. Model Sharing Agreements. 12

Chapter 6—MODEL GOVERNANCE **15**

6.1. Model Governance. 15

Chapter 7—ROLES AND RESPONSIBILITIES **16**

7.1. STARCOM Command Data and Artificial Intelligence Officer (CDAO). 16

7.2. HQ STARCOM Directors/Delta Commanders. 16

7.3. HQ STARCOM Judge Advocates (JA). 17

7.4. HQ STARCOM Intelligence Directorate (S2). 17

7.5. HQ STARCOM Operations Directorate (S3). 17

7.6. HQ STARCOM Cyber Security (S4/6). 17

7.7. HQ STARCOM Plans, Programs, and Requirements (S/5/8/9). 18

7.8. Test Directors and Model Developers. 18

7.9. Model Managers. 18

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION **19**

Attachment 2—MODEL STANDARDS AND FRAMEWORKS **25**

Attachment 3—MODEL LIFECYCLE MANAGEMENT **33**

Attachment 4—MODEL SHARING AGREEMENT TEMPLATE **41**

Attachment 5—MODEL FIDELITY, CREDIBILITY AND RISK MANAGEMENT **44**

Chapter 1

MODEL MANAGEMENT

1.1. Background. The USSF's vision as a Digital Service is to be an interconnected, digitally dominant force that leverages cutting-edge innovation and technology to outpace the adversary. In achieving this vision, Space Training and Readiness Command (STARCOM) must aggressively close the gap between the real-world operational space environment and its' virtual, digital representations. The STARCOM Digital Range (S-DR) is a physics-defined digital representation of the space domain where capability-based models are integrated to support Test, Training, and Exercise (TT&E) events. TT&E events rely on digital models to simulate how actual capabilities will perform in the real space environment. The ways in which the FLDCOM performs its missions must include revolutionary innovative and technological shifts to fight and win within a continuously evolving warfighting domain. This instruction outlines the management of digital models.

1.2. Model Management (MM). Digital model management is a structured organizational approach to optimize the utility of model assets and their associated data. This approach includes an overarching governance framework, policy and guidance, and defined processes for developing, verifying, validating, accrediting, certifying, tracking, sustaining, sharing, storing, and decommissioning models. Digital models are data assets that must be properly managed to improve mission effectiveness, readiness, lethality, and investment decisions. STARCOM digital models are managed at the Headquarters' level to ensure consistent management processes; models are Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure (VAULTIS); and digital model development aligns to an interoperable "plug and play" digital space environment. VAULTIS promotes model discovery via tagging and cataloging, model sharing and reuse minimizing redundancy, and accessible model derived insights via authoritative and traceable data sources used in training, testing, and validation. Interoperable models (e.g., spacecraft, ground stations, tactical mobile ground space systems, etc.) permit a simultaneous optimization of modeled assets supporting dynamic and complex TT&E events and analysis.

Chapter 2

MODEL TYPES

2.1. Model Types. A model is a physical, mathematical, or logical representation of an actual or conceptual system, entity, phenomenon, or process. Models may include requirements, design, analysis, and validation data. Digital models are multi-dimensional representations of a physical object, system, or phenomenon generated by computer software for analysis, simulation, and/or visualization. Digital Twins (DT) and Artificial Intelligence (AI) models are specific types of digital models. A digital twin is a dynamic, virtual representation of a physical object, process, or system that mirrors its real-world counterpart in near-real time. Communication occurs between real space assets and their digital twin by leveraging a digital ecosystem of sensors, networks and data. Connecting the real and virtual worlds allows for continuous, near-real time data flow and synchronization. Digital twins enable continuous monitoring, simulation, analysis, and prediction of performance regarding their real-world counterpart. Digital twins may vary in fidelity, based on the use case. An AI model is a software program or algorithm trained on vast datasets to recognize patterns, make predictions, or generate content autonomously. This instruction applies to all types of digital models.

2.2. Digital Models (DM) Per DoD Instruction 5000.97:

2.2.1. Identify and maintain model-centric baselines, approaches, and applications in a digital form that integrates the technical data and associated digital artifacts that stakeholders generate throughout the system life cycle. Develop digital model(s) using standard and best practice model representations, methods, and underlying data structures to maximize interoperability.

2.2.2. Establish a standard approach for developing each type of digital model. Consider the use of existing modeling standards and approaches to improve integration of models across the Department of War (DoW). Evaluate all digital models to ensure they are accurate, complete, trusted, and reusable. Develop digital models in accordance with applicable DoW policies, guidance, and standards. Reference the Acquisition Streamlining and Standardization Information System (available at **https://assist.dla.mil/online/start**) and DoW Information Technology Standards Registry repositories as government-adopted authoritative sources of truth for standards.

2.2.3. Update and maintain the digital model(s) throughout the system life cycle and maintain configuration management (i.e., version control). These updates, conducted within the digital models, will provide stakeholders, including digital model developers, simulation users, testers, and other engineering and management personnel, with the ability to extract and analyze consistent and up-to-date system information. Digital models and simulations must be updated using all relevant real-world data throughout the system life cycle since they will be used to make decisions, inform manufacturing, generate software code, etc.

2.2.4. Ensure digital models, simulations, and associated data are Verified, Validated, and Accredited (VV&A) for their intended use, in accordance with DoDI 5000.61.

2.2.5. Authoritative Data. Develop and implement plans to establish current, consistent, enduring, and authoritative sources of truth for digital models and data. See the DoD Data Strategy for additional information on data attributes, including achieving VAULTIS goals.

2.3. DT/AI Models. DT development involves creating virtual replicas of physical assets, systems, and even human performance to enhance design, training, maintenance, and decision-making across the entire defense acquisition lifecycle. DT development may leverage AI, cloud computing, and authoritative data sources to continuously synchronize with its physical counterpart through a continuous "digital thread" of data, enabling real-time monitoring and updates. The digital thread enables leaders with real-time insights by continuously monitoring assets and automatically retraining machine learning (ML) algorithms to adapt to changing conditions and threats.

2.3.1. Accreditation. Digital models may only be used in official training or test events with formal accreditation by the appointed authority. Accreditation is the command's endorsement that a model is acceptable for specific use. Given the adaptive nature of AI models and the complexity of DTs, accreditation shall be use-case-specific. The model is approved for a defined scope or context (e.g., "satellite proximity operations training at unclassified level"), and any use outside that scope requires a new risk assessment or re-accreditation. The accreditation decision (documented via memo or certificate) will be stored with the model's metadata along with all supporting V&V evidence.

2.3.2. Versioning and Re-Accreditation Triggers. Any significant update to a digital model (e.g., new training data, a major algorithm change) or to a digital range component (e.g., integrating a new sensor feed, a major fidelity upgrade) shall result in a new model version release. The model registry must track these versions, and importantly, a major version change *invalidates* the prior accreditation. The updated model must undergo a partial re-validation, and the VV&A Authority must determine whether re-accreditation is required before the new version is operationally used. Thresholds for what constitutes a "significant change" should be defined in the VV&A Plan; however, as a rule, any change that affects the model's outputs beyond the established uncertainty budget or that alters the model's intended use shall trigger re-accreditation review. Additionally, time-based re-validation should be enforced for AI models: if an AI model has not been updated or re-evaluated within a certain period (for example, 2 years), it must be reviewed for drift and re-affirmed or re-accredited as needed to ensure it still meets performance criteria. The review should be independently performed by an assigned individual, group, or entity not associated with the development of the model of interest.

2.3.3. Digital Product Support. Digital product support is the package of support functions required to field and maintain the readiness and operational capability of covered systems, subsystems, and components, including all functions related to covered system readiness. STARCOM leverages digital engineering methods, digital data and system models to implement the Product Support Strategy, enable data-driven decision making, and deliver effective and efficient product support outcomes throughout the system lifecycle.

2.3.4. Wherever DT/AI models are used, additional management controls are required to instill trust and ensure safety. At a minimum, each DT/AI model (or AI-enabled component) in STARCOM's model catalog shall include:

2.3.4.1. Model Card Documentation. A Model Card is a concise document capturing the model's intended use, development data and provenance, architecture, training data sources, limitations, assumptions, performance metrics, and known limitations. Model cards shall be stored with the model's metadata so any user can readily understand the

model's purpose and credibility before use. *(This implements the "rigorous model documentation" measure identified in STARCOM's DT/AI governance approach).*

2.3.4.2. Training and Evaluation Lineage. The origin of the model's behavior must be traceable. All DT/AI models will have records of their training datasets, training methodology, and test evaluation results. The metadata shall reference the data sources or simulators used to develop the model, along with key validation statistics (e.g., accuracy, error rates). This lineage is part of the model's VV&A evidence, enabling reviewers to assess whether the model was trained on relevant and sufficient data for its intended use.

2.3.4.3. Bias and Uncertainty Characterization. Any biases, uncertainties, or error margins in the model's outputs must be characterized and documented (typically in the model card). For example, if an DT/AI space threat model is less accurate in certain orbital regimes or has a known false alarm rate, those limitations shall be disclosed. During V&V validators will establish acceptable error bounds (an uncertainty budget) for the model and ensure the model meets required fidelity within those bounds. This defines quantitatively how much error is tolerable for the model's outputs and guides both accreditation and future re-calibration efforts.

2.3.4.4. In addition to the above controls, all DT/AI models shall undergo an operational test for their intended use before accreditation. This validating must include the successful execution of one or more Government-approved "golden scenarios". A *golden scenario* is a benchmark test case, often derived from a historical event or a high-priority mission use-case, with a known or expected outcome. Its' successful execution serves as the gold standard for validating a model's performance in a mission-relevant context. The model must demonstrate acceptable performance in this context prior to being accredited for official use. For example, before accrediting an AI model that predicts spacecraft conjunctions, it should be tested against a known historical conjunction event (the golden scenario) to verify it can predict collision risk within required error margins. These requirements tie directly into the VV&A process: the VV&A Plan for a DT/AI model will enumerate the required documentation (model card, data sources), the acceptance criteria (uncertainty budget, bias checks), and the test plan (including golden scenarios for validation). Likewise, the model's metadata entry will include fields tagging it as an "AI" model and linking all the above artifacts (documentation, test results, etc.). By enforcing these measures, STARCOM ensures that any AI-driven models are transparent, well-understood, and under continuous oversight. This governance is consistent with DoW Responsible AI principles (requiring transparency, traceability, etc.) and is essential for warfighter trust in AI-enabled simulation.

Chapter 3

MODEL STANDARDS

3.1. Model Standards. All digital model artifacts must fit into the standard modeling and architecture taxonomy defined in **Attachment 2**. STARCOM will not treat digital models as exotic, stand-alone tools; rather, they are part of the broader enterprise of M&S, and thus subject to the same interoperability and standards requirements. Department of Defense Architecture Framework (DoDAF) and/or Unified Architecture Framework (UAF) architectural frameworks and modeling languages (Systems Modeling Language (SysML), Unified Model Language (UML), etc.) will be used to describe digital models. The inclusion of DT/AI models adds new content to the architecture, but not a new structure, existing standard architecture views will be used to describe them.

3.2. Taxonomy. Consistent taxonomy also means there is a digital model registry and standards hierarchy (see **Attachment 2**) will have "identifiers" or categories for DT/AI models. Taxonomy categorizes models by domain (orbital mechanics, communications, threat, etc.) and by type (constructive simulation, hardware-in-the-loop, analysis model, etc.). AI models that are part of a larger system model and DTs should be placed in this taxonomy based on their function and domain.

3.3. Standards Compliance. Data or model interchange involving DT/AI models must align with open standards where possible, for example, using Space Force-approved data schemas for orbit ephemerides, or Open Application Programming Interface (OpenAPI) for simulation services, to prevent proprietary AI "black boxes" from undermining interoperability. Guidance on model encoding (use of open formats, XML/XMI for metadata, etc.) to be heeded by DT/AI model developers as well. Finally, when a model is formally accredited and adopted, and calls for designating an authoritative model-of-record in the catalog. As noted above, a DT/AI model that earns model-of-record status for a specific purpose will be flagged in the registry with the VV&A Authority's approval. The taxonomy will thus clearly show which DT/AI model is the approved standard for its niche. Ensuring DT/AI models are fully integrated into the existing standards and taxonomy framework guards against them becoming isolated stovepipes; instead, they enrich the overall digital ecosystem while remaining visible, understandable, and interoperable components of STARCOM's model inventory.

3.4. MOSA and Open Interfaces. Digital model components will use published, open interface control documents and enterprise data schemas to ensure plug-and-play interoperability and avoid proprietary lock-in.

3.5. Interoperability Verification. Prior to accreditation, models shall demonstrate conformance to the connection profile (timing, control and data interfaces) and record results in the VV&A package.

3.6. Standardized Model Interface (SMI). Digital models must adhere to SMI to ensure interoperability and integration within the S-DR. This interface is the sole approved method for models to publish their actions to the environment and subscribe to effects from the S-DR's Core Physics and Propagation Services.

Chapter 4

MODEL CATALOGING, METADATA, AND STORAGE

4.1. Cataloging. Digital models will be visible and accessible except where constrained by law, regulation, security classification, guidance, or policy. Model constraints may include but are not limited to Personally Identifiable Information (PII) protected pursuant to Title 5 United States Code (USC) Section (§) 552a, Records maintained on individuals (also known as the Privacy Act of 1974); individually identifiable protected health information (PHI) according to Section 264 of Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996*; information exempted from mandatory public disclosure in accordance with 5 USC § 552, Public information; agency rules, opinions, orders, records, and proceedings (the Freedom of Information Act (FOIA)); information within systems covered under attorney-client privilege or attorney work product; information restricted from release due to security classification; and information controls on secondary release and dissemination of technical documents and data marked with the distribution statements required by Department of Defense Instruction (DODI) 5230.24, *Distribution Statements on DoD Technical Information.*

4.1.1. Model products and outputs generated from testing, training, and evaluation to be labeled and cataloged, maintaining versioning history and ensure proper association with the intended applications.

4.1.2. Model Type. To support catalog search and discovery, of registered models, identify the model's category, e.g., "AI," "Physics-Based," "Environment DT," or "Hybrid" model.

4.1.3. Catalog Alignment. Digital model entries shall include the Environment Baseline Version and Model-of-Record flag (when assigned) to align catalog metadata with taxonomy and interface standards.

4.2. Metadata Tagging.

4.2.1. Digital models will be visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset. Metadata standards will be in accordance with DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense.*

4.2.2. Metadata for models will federate to higher level agency catalogs as requested and/or be registered in an approved STARCOM data and/or model catalog whenever a model catalog is available and/or provided. The catalog relies on metadata to describe the model, enabling users to search, understand, and access a model. Metadata provides users with accessible information about the model, including details beyond their specific domains. Using metadata also enables assessments of model sharing and usage throughout the organization. STARCOM will drive model sharing and reuse through cataloging and exposure of robust model metadata tagging, model stewardship, and processes for ensuring a common understanding of our models. Every model and simulation will be tagged with a unique identifier and version.

4.2.3. At a minimum, digital models will be identified and tagged with their security metadata, to include the classification determination, markings, disclosure, and handling rules to support access control in accordance with DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*.

4.2.4. All instances of PII and PHI in the data sources will be identified and tagged.

4.2.5. All information required for records management (Privacy Act information, essential records indicator, FOIA Exempt Indicator, storage and archive information, preservation information, tracking information, disposition information including date to dispose of, etc.) will be identified and tagged in accordance with AFI 33-322.

4.2.6. Metadata for DT/AI Models. DT/AI models introduce new metadata considerations beyond those previously discussed; these models shall be cataloged in central model registries with additional metadata fields to capture their unique attributes. At a minimum, the following fields or tags will be recorded for each DT/AI model (in addition to the standard metadata defined in **Paragraph 3.2**.):

4.2.6.1. Environment Baseline Version. *(For digital models linked to the S-DR baseline only).* Specify the STARCOM S-DR version or dataset release to which this digital model corresponds. This ties any scenario or result to the exact environment configuration used.

4.2.6.2. Model Version and/or Identifier. A unique version number or immutable identifier (e.g., a hash) for the specific model instance. For AI software models, a hash of the model file or weights shall be recorded. This ensures that the exact version used in VV&A evidence or events can be verified.

4.2.6.3. Training Data Provenance. *(AI models only.)* A description or pointer to the data sources used to develop or train the model. For example, "Trained on orbital tracking data from 2015–2024 and 100 simulated conjunction scenarios." The entry should reference dataset IDs in the repository or external data archives as applicable.

4.2.6.4. Evaluation Metrics. Key performance metrics and validation results achieved by the model, including, but not limited to, accuracy, precision, recall, F1-score, measure of performance; mean absolute error (MAE), root mean squared error (RMSE), R-squared (for regression); and metrics related to fairness, stability, and explainability. For instance, "95% classification accuracy on test set X; orbit propagation error ≈ 1 km over 24 hours." This summary captures the model's validated capability and fidelity in quantitative terms.

4.2.6.5. Intended Use and Limitations: A concise statement of what the model is *approved* for and any known limitations. For example: "Intended for unclassified training only; not validated for predictive operations," or "Valid for altitudes below 500 km; accuracy degrades for higher orbits." This should align with the model's accreditation scope and is drawn from the model card and accreditation documentation.

4.2.6.6. VV&A Evidence Links. References to all pertinent VV&A artifacts for this model, such as the VV&A Plan identifier, test reports, validation datasets, accreditation letter reference, and scenario result archives. The metadata system shall allow attaching or linking these documents so that a user can drill down into how the model was verified and validated.

4.2.6.7. Software Bill of Materials (SBOM) and/or Dependencies. For software-based models (especially AI), include a link or file listing the SBOM (and Hardware BOM, if applicable) for the model. This provides transparency into third-party libraries, packages, and hardware components, which is crucial for cybersecurity and sustainment (e.g., tracking if a library has known vulnerabilities or requires update).

4.2.6.8. Classification and Releasability. The security classification and distribution controls for the model and its data. For example, a model might be Controlled Unclassified Information (CUI, SECRET/NOFORN, etc.). This is important because some AI models might be unclassified code but trained on sensitive and/or proprietary data, proper markings ensure the model is handled and shared in accordance with its content (per §3.2.1 tagging policy). Any classified or CUI information (to include technical data) to allies and foreign partners is bound by foreign disclosure procedures IAW DAFMAN 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program*. If a model is trained using Classified Military Information (CMI) or CUI information, the source information will need to go through this process to ensure the model is handled and shared in accordance with its content.

4.2.6.9. Model-of-Record Status. An indicator if the model has been designated as the official Model-of-Record in its domain or category. Only one model per domain/function is typically endorsed as the authoritative "model-of-record" for that purpose. Model tagging enforces that only one model in each category carries this designation at a time. The Model-of-Record indicator in the registry highlights which model is the authoritative standard in a given area, improving clarity for users searching the catalog.

4.2.6.10. Metadata extensions shall be incorporated into the model catalog schema. They ensure that anyone discovering a model in the registry can immediately recognize it as an "DT" or "AI" model and understand its pedigree and limitations before reuse. The additional tags also facilitate enterprise management tasks, for instance, tagging a model with "AI-enabled" or "DT" allows quick filtering for all such models (and applying any special access controls if needed).

4.2.6.11. Metadata and Lineage Tracking. Lineage tracking is accomplished to trace each deployed model back through its training data, underlying algorithms, and validation results, as well as to trace forward into which system build or scenario it was used in. This traceability ensures accountability and supports configuration control. Configuration control maintains the digital thread of model updates, linking requirements to models to test results to operational performance, thereby providing stakeholders an authoritative record of model evolution. In practice, when a model is updated (e.g., retrained with new data), a new model card is generated and versioned for audit and traceability. The history of changes (datasets used, parameters, validation outcomes) is also recorded, and previous versions of both the model and its' card are archived. This metadata and lineage information allows the developer to answer that question "which model version was used for this result, and where did it come from?", a crucial capability for troubleshooting and governance.

4.3. Model Storage. STARCOM MM requires the models to be stored in approved environments and at the appropriate classification level.

Chapter 5

MODEL SHARING

5.1. Intra-Service Model Sharing.

5.1.1. Inter-Service or Inter-Agency Model Sharing. All models shared between the DAF and one or more DoW Components, non-DoW federal agencies, or federally recognized organizations will be exchanged and/or managed as prescribed by a Memorandum of Agreement (MOA), in accordance with AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures.* Data collected or created in pursuit of independent research and development will also be managed in accordance with DoDI 3204.01, *DOD Policy for Oversight of Independent Research and Development (IR&D).*

5.1.2. Other Model Sharing. All other model sharing to include sharing with one or more State or local governmental agencies, industries, or academia, must comply with applicable laws, regulations, and policy. STARCOM members must contact the servicing judge advocate for guidance on applicable laws, regulations, and policies prior to entering a model sharing agreement.

5.2. Model Sharing Agreements.

5.2.1. Visible and accessible models do not require a model sharing agreement.

5.2.2. Models will be shared unless an exception is approved by the FLDCOM Chief Data Officer per Judge Advocate (JA) counsel. Exception considerations include but are not limited to legal constraints, regulations, security classification, guidance, policy and/or identified adverse effects to DAF missions. Approval authority will not be delegated.

5.2.3. Model sharing agreements detail the processes, procedures, and sharing of models between organizations (reference **Attachment 4** for additional information), to include allies and mission partners. At a minimum, all STARCOM model sharing agreements will document the following:

5.2.3.1. List the parties entering into agreement (organization names and contact information for primary and alternate points of contact).

5.2.3.2. Identify the legal authority leveraged and the reasons for entering into the model exchange to make the model exchange permissible.

5.2.3.3. Outline the responsibilities and obligations of the agreement parties, including addressing third- party rights and responsibilities.

5.2.3.4. The model and supplemental information must be requested.

5.2.3.5. The method for model sharing must include details about the supplying and receiving system or model platform.

5.2.3.6. Frequency at which models will exchange, update, or backup.

5.2.3.7. Model owner’s access to information and decision rights following any exchange.

5.2.3.8. Security and access control requirements for model exchange and receipt, including how access control will be audited for the record. Agreements that result in the sharing of US CMI or CUI with allies and foreign mission partners must go through the

DAF foreign disclosure process and be approved for release to specified allies/foreign partners IAW DAFMAN 16-201.

5.2.3.9. Timely reporting of incidents affecting model covered by the agreement.

5.2.3.10. Resource impacts for implementing model sharing.

5.2.3.11. Methods for mitigating risk and resolving disputes.

5.2.3.12. Terms for terminating the agreement, or transference, and any notice period will be required.

5.2.3.13. Model Sharing Agreements will be managed by and reside with the Chief of Staff (CoS) office.

5.2.4. DT/AI Model sharing. Additional clauses are required when sharing DT/AI models between organizations. The Model Sharing Agreement shall include provisions addressing the special risks and requirements of DT/AI models. Specifically, when sharing a DT/AI model between STARCOM and an external entity, the following shall apply:

5.2.4.1. Verification and Documentation. The providing organization must affirm that the model has been verified and validated for its intended use and shall furnish the receiving organization with the model's VV&A documentation (at minimum, the model's accreditation report and its model card). This ensures the receiver has evidence of the model's credibility and approved use-case.

5.2.4.2. Use-Boundaries. The receiving organization must agree to employ the model only within its validated scope of use, unless they conduct further VV&A to accredit it for a new use. In other words, the model will not be repurposed beyond what it was cleared for (e.g., using a training-only AI model in an operational analysis) without additional verification and accreditation by the receiver.

5.2.4.3. Dependencies and Openness. The provider shall supply any necessary runtime dependencies (such as AI model files, libraries, or supporting environment data) along with a SBOM for transparency. This ensures the receiver can integrate the model into their environment (their S-DR instance or equivalent) in a modular, open manner. It aligns with MOSA principles and prevents vendor lock-in or black-box integration.

5.2.4.4. Incident Reporting and Rollback. Both parties shall include an incident reporting and rollback clause. If the model exhibits unexpected or unsafe behavior in use, the receiver will promptly notify the provider and STARCOM's VV&A Authority and will cease use (rollback to a previous stable version or other approved backup) as directed. This binds external use of the model to the same safety net procedures that STARCOM uses internally, ensuring issues are communicated and the model can be pulled from use if it fails.

5.2.4.5. The terms to model exchange agreements and the sharing of DT/AI models will uphold the same level of assurance and control as internal use. STARCOM's model governance and risk management practices thus extend to any external model collaborations or transfers.

5.2.4.6. The DT/AI model provider shall include VV&A evidence (VV&A plan/report, accreditation memo and a model card with stated uncertainty bounds), runtime dependencies, and SBOM and/or HBOM. The receiver shall use the model only within its

accredited intended use; employing a model outside that scope requires additional VV&A and a new accreditation decision; and promptly report any incidents to the provider and VV&A Authority, cease use, and rollback to the last accredited version when directed; record the incident and action for VV&A review.

Chapter 6

MODEL GOVERNANCE

6.1. Model Governance. Model governance is a structured framework comprised of people, policies, processes, and roles and responsibilities to manage the entire lifecycle of a digital model. STARCOM governance bodies (Working Groups, Boards, and Councils) are developed and implemented to ensure consistency of model management activities across the FLDCOM, USSF, DAF, and DoW enterprises. Model governance facilitates the delivery of the right data and models to the right user at the right place at the right time.

6.1.1. Governance bodies (Working Groups, Boards, and Councils) support Subject Matter Experts (SMEs), Action Officers (AO), leadership and stakeholder cross-communication, awareness, and decision-making regarding issue Courses of Action (COAs) and directed actions and/or resolution measures.

6.1.2. Model governance and management activities foster an environment suitable for optimal mission performance by promoting accountability for models as enterprise assets and enabling efficient collaboration among necessary stakeholders. Model management SMEs and AOs shall present model management issues to the STARCOM Data Management Working Group, Board, and Council (as needed) for resolution.

6.1.3. Governance bodies also oversee the S-DR baseline control and model incident and/or rollback coordination, synchronizing decisions among the VV&A Authority.

Chapter 7

ROLES AND RESPONSIBILITIES

7.1. STARCOM Command Data and Artificial Intelligence Officer (CDAO).

7.1.1. Serve the STARCOM Commander to establish, maintain, approve, and oversee FLDCOM MM guidance development, execution and approve compliance waivers to this instruction.

7.1.2. Participate in and leads MM Governance Forums. Establish and lead the STARCOM Data Management Working Group (DMWG) and Board. Present model management-related topics, issues, and products to be elevated and/or addressed at higher governance levels (STARCOM Board and Council) as needed.

7.1.3. Act as a liaison for STARCOM to integrate the operation and management of model sharing in support of strategic and operational capabilities and informed decision-making. Communicate plans and execute model management to ensure models are VAULTIS.

7.1.4. Facilitate execution of model sharing agreements before models are shared outside the DAF.

7.1.5. Ensure model tagging in accordance with USSF policies and implementation guidance.

7.1.6. Ensure FLDCOM TT&E model catalogs are developed and sustained at each appropriate classification level of the S-DR.

7.1.7. Ensure model tagging, retention, and secure handling standards.

7.1.8. Ensure enterprise and/or approved platforms for model storage.

7.1.9. Ensure the development and maintenance of the S-DR, include its Core Physics and Propagation Services and Dynamic Environment Controls; publish interface standards; manage configuration-controlled releases; coordinate fidelity updates and data rights; propose model-of-record selections for final VV&A Authority approval; and ensure all STARCOM TT&E events use the current S-DR baseline.

7.1.10. Ensures blue space models for development are part of the Comprehensive Cost and Requirement System (CCaRS) Model Management Workflow for coordination and/or approval.

7.1.11. Lead implementation and oversight of this guidance.

7.2. HQ STARCOM Directors/Delta Commanders.

7.2.1. Provide SMEs, AOs, stakeholders, and leadership to present MM issues at the appropriate levels, to the Data Management Working Group, Board, and Council.

7.2.2. Ensure models are VAULTIS.

7.2.3. Implement this model policy and standards that enable the use of federated enterprise capabilities.

7.2.4. Leverage the command model catalog/s.

7.2.5. Leverage enterprise and/or approved platforms for model storage.

7.2.6. Enforce model tagging, retention, and secure handling standards.

7.3. HQ STARCOM Judge Advocates (JA). Advises on all legal matters related to model and data management, governance, use, and sharing activities.

7.4. HQ STARCOM Intelligence Directorate (S2).

7.4.1. The Director of S2 serves as the approval authority for all STARCOM space threat models, simulations and scenarios throughout the Intelligence Community (IC) VV&A Process. Approval authority may be delegated.

7.4.2. Provide SME, AOs, stakeholders, and leadership to present space threat models, scenarios and information at the appropriate levels, to the Data Management Working Group, Board and Council.

7.4.3. Provide IC-validated space threat models, scenarios and information in support of M&S requirements per the VV&A process, IAW SPFI 16-1002.

7.4.4. Provide intelligence oversight in support of MM and throughout the IC VV&A process.

7.4.5. Liaise with the IC to ensure IC/space threat models meet STARCOM integration requirements (format, fidelity, lineage, releasability) for use within S-DR for TT&E.

7.4.6. Space Threat Model Awareness. Facilitate and liaison the use and access to space threat models employed in S-DR.

7.5. HQ STARCOM Operations Directorate (S3).

7.5.1. Acts as the STARCOM space blue model VV&A certification authority, reviews model development documentation and accredits space blue models as the lead for the STARCOM Model Approval Process, serves in the governance process to review and/or approve compliance waivers to this instruction with the STARCOM CDAO.

7.5.2. Convenes expert panels as needed and may suspend or withdraw a model's accreditation if risk or performance issues emerge.

7.5.3. Serve as the operations liaison to USSF Combat Forces Command (CFC), Space Systems Command (SSC), and other USSF elements to ensure S-DR interface and/or standards compliance for operational models and integration.

7.5.4. Ensure each exercise and test plan declares the S-DR baseline and specific space blue model versions prior to start-of-event and verify rollback procedures are in place.

7.5.5. Ensure all required metadata is captured for all space blue models (e.g., model cards, training data sources, SBOMs) and apply any access controls or caveats based on classification and releasability. Coordinate with Cybersecurity to address any software vulnerabilities identified via SBOM analysis before the model's release for use.

7.6. HQ STARCOM Cyber Security (S4/6).

7.6.1. Evolve, establish, manage, and make available the enterprise services and the interface standards and specifications for the sharing of models, data, information, and IT services to meet the needs of the STARCOM Components and their validated enterprise requirements.

7.6.2. Ensure information technology architectures meet model capacity requirements (when running) for latency and bandwidth requirements.

7.7. HQ STARCOM Plans, Programs, and Requirements (S/5/8/9).

7.7.1. Through the appropriate S5/8/9 corporate processes prohibit the programmatic planning across the Future Years Defense Programs (FYDP) of funds and manpower billets for model development programs, projects, and initiatives that do not comply with this instruction and/or have not obtained a compliance waiver to this instruction via HQ STARCOM/S3 and the STARCOM CDAO office.

7.7.2. Provide mechanisms to ensure STARCOM data, information, and IT services under the Command Special Access Program Management Office (SAPMO) are properly registered, exposed, and available and secure.

7.7.3. In coordination with the STARCOM SAPMO and STARCOM CDAO, adjudicate waivers and change requests submitted by STARCOM Components.

7.8. Test Directors and Model Developers.

7.8.1. Ensure models are versioned, annotated, and preserved per model lifecycle management policies.

7.8.2. Ensure all models are approved for government use and are built in accordance with government policy.

7.9. Model Managers.

7.9.1. Serve as the custodian of the STARCOM model repositories and catalogs. Update the metadata schema to include all new DT/AI fields (model type, version IDs, SBOM links, etc.) and ensure every model entry, especially DT/AI models, are populated with this information.

7.9.2. Verify that the model provider has included a model card, training data description, VV&A documentation, and SBOM as required; flag any omissions to the model owner and VV&A Authority as new models or updates are submitted.

7.9.3. Manage access controls in the catalog. Enforce classification and releasability rules for models (for example, restrict AI models trained on sensitive data to authorized users).

7.9.4. Coordinate with cybersecurity personnel to record vulnerability assessment results (e.g., note in the catalog if a model's SBOM was cleared or if certain components need patching).

7.9.5. Archive superseded model versions rather than deleting, maintain the digital thread by linking older versions and their validity dates in the system, so nothing is lost and rollback is possible when needed.

MATTHEW S. CANTORE
Brigadier General, USSF
Deputy Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 USC § 552, Public information; agency rules, opinions, orders records, and proceedings (the Freedom of Information Act

5 USC § 552a, Records maintained on individuals (the Privacy Act of 1974)

44 USC § 3502, Definitions

AFI 16-1001, *Verification, Validation and Accreditation (VV&A)*, 29 April 2020

AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures,*18 October 2013

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFPD 90-70, *Enterprise Data Management*, 13 February 2020

CJCSI 5123.01J, *Charter of the Joint Requirements Oversight Council and the Joint Force Requirements Process*, 15 January 2026

DAFMAN 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program*, 19 January 2021

Data Management Association, *Data Management Body of Knowledge* (2nd Edition), July 2017

DoDD 3100.10, *Space Policy*, 30 August 2022

DoDI 3204.01, *DoD Policy for Oversight of Independent Research and Development (IR&D)*, 20 August 2014

DoDI 5000.61, *DoD Modeling and Simulation Verification, Validation, and Accreditation*, 17 September 2024

DoDI 5000.70, *Management of DoD Modeling and Simulation (M&S) Activities*, 10 May 2012

DoDI 5000.82, *Requirements for the Acquisition of Digital Capabilities*, 1 June 2023

DoDI 5000.87, *Operation of the Software Acquisition Pathway*, 2 October 2020

DoDI 5000.88, *Engineering of Defense Systems*, 18 November 2020

DoDI 5000.97, *Digital Engineering*, 21 December 2023

DoDI 5230.24, *Distribution Statements on DoD Technical Information*, 10 January 2023

DoDI 5400.11, *DoD Privacy and Civil Liberties Programs,* 29 January 2019

DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense,* 5 August 2013

DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense,* 3 August 2015

DoDI 8330.01, *Interoperability of Information Technology, Including National Security Systems*, 27 September 2022

DoDM 5000.102, *Modeling and Simulation Verification, Validation, and Accreditation for Operational Test and Evaluation and Live Fire Test and Evaluation*, 9 December 2024

Executive Office of the President, *The Common Approach to Federal Enterprise Architecture,* 2 May 2012

MIL-STD-3022, *Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations*, 9 February 2026

PL 104-191, *Health Insurance Portability and Accountability Act of 1996*, 21 August 1996

SPFI 16-1002, *Threat Modeling, Simulation, and Analysis Guidance*, 20 November 2025

STARCOMI 90-700, *Data Management*, 12 August 2025

Abbreviations and Acronyms

AFI—Air Force Instruction

AI—Artificial Intelligence

AO—Action Officer

API—Application Programming Interface

ASSIST—Acquisition Streamlining and Standardization Information System

CCaRS—Comprehensive Cost and Requirement System

CDAO—Command Data and Artificial Intelligence Officer

CDOC—Chief Data Officer Council

COA—Course of Action

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DE—Digital Engineering

DMWG—Data Management Working Group

DoD—Department of Defense

DoDAF—Department of Defense Architecture Framework

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoW—Department of War

DTD—Digital Twin Description

FLDCOM—Field Command

FOIA—Freedom of Information Act

FYDP—Future Years Defense Programs

HBOM—Hardware Bill of Materials

IPO—Integrated Program Office

IT—Information Technology

LLM—Large Language Model

MM—Model Management

MOA—Memorandum of Agreement

MOSA—Modular Open Systems Approach

M&S—Modeling and Simulation

OPEN—Open, Public, Electronic, Necessary

OPR—Office of Primary Responsibility

OTTI—Operational Test and Training Infrastructure

PII—Personally Identifiable Information

PHI—Protected Health Information

SAPMO—Special Access Program Management Office

SBOM—Software Bill of Materials

SDP—Space Doctrine Publications

SPFI—Space Force Instruction

SME—Subject Matter Expert

STARCOM—Space Training and Readiness Command

S-DR—STARCOM-Digital Range

T&E—Test and Evaluation

TT&E—Test, Training and Evaluation

USSF—United States Space Force

VAULTIS—visible, accessible, understandable, linked, trustworthy, interoperable, and secure

VVA—Verification, Validation, and Accreditation

Office Symbols

OTTI/IPO—Operational Test and Training Infrastructure Integrated Program Office

STARCOM/CDAO—Command Data and Artificial Intelligence Office

STARCOM/JA—Judge Advocates

STARCOM S3—Operations

STARCOM/S4/6—Cyber Security

STARCOM/FM—Financial Management

Terms

Accessible—Data and services can be accessed via the Global Information Grid by users and applications in the enterprise. Data and services made available to any user of applications, except where limited by law, policy, security classification, or operational necessity (Ref: DoD Information Enterprise Architecture Version 3.0; AFI 17-140).

Architecture—A systematic approach that organizes and guides design, analysis, planning, and documentation activities. (*The Common Approach to Federal Enterprise Architecture*, May 2012).

Artificial Intelligence—Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. An artificial system designed to think or act like a human, including cognitive architectures and neural networks. A set of techniques, including machine learning that is designed to approximate a cognitive task. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting. (*The National Defense Act of 2019, EO 13960, Section 238(g)*).

Board—A panel of individuals, typically officers, enlisted personnel, or civilians, who convene to make decisions regarding specific matters. Boards are convened at the Colonel or equivalent level, Senior-leader decision making level.

Capability—The ability to complete a task or execute a course of action under specified conditions and level of performance (CJCSI 5123.01J), and physical representation of data.

Council—A panel of individuals, typically Executive-level officers, enlisted, or civilian personnel who convene to make decisions regarding specific matters.

Councils are convened at the General Officer or equivalent level, Executive—leader decision making level.

Data—Recorded information, regardless of form or the media on which it is recorded (44 USC § 3502).

Data Architecture—Defines the blueprint for managing data assets by aligning with organizational strategy to establish strategic data requirements and designs to meet the requirements (Ref: Data Management Association – Data Management Body of Knowledge (DAMA DMBOK) 2nd Edition). Includes abstraction, conceptual, logical, and physical models; high-level data concepts and their relationships; data requirements; data structures; and metadata models. (CJCSI 5123.01J).

Data Asset—A collection of data elements or data sets that may be grouped together (44 USC § 3502).

Data Catalog—A set of information describing the contents, format, and structure of a database, and the relationship between its elements; used to control access to and manipulation of the database.

Data Officer—An empowered designee selected by the directorate that will facilitate the sharing of Department of the Air Force data across the enterprise.

Data Source—origin of data, such as a database, file, voice, video, imagery etc.

Data Standards—A documented agreement and specification by an authoritative body on a definition, representation, or format of data, metadata, or exchange protocol that is used to improve data understanding and data interoperability. A data standard requires a narrative specification and may include complementary data engineering resources to guide IT system development and testing conformance. Widespread adoption of a well-designed data standard can reduce ambiguity and the necessity for mediation, while promoting efficiency and transparency of mediation as required (Ref: DoDI 8320.07).

Digital Cousin—A simulation run where a validated digital model is executed within an environment where one or more parameters (e.g., environmental conditions, system performance characteristics) have been deliberately perturbed from their baseline values. The execution of thousands of these "cousins" in a robustness campaign is used to test a system's design resilience against a wide range of off-nominal conditions.

Digital Model—A digital (i.e., in an electronic form, able to be read and manipulated by computer) representation of an object, phenomenon, process, or system. The representation can include form, attributes, and functions and may be depicted visually or described via mathematical or logical expressions. (Defense Acquisition University Glossary).

Digital Range—The authoritative, government-controlled environment used for all STARCOM Test, Training, and Exercise (TT&E) events. Architecturally, it is a single synthetic digital model of the space environment hosted on information systems accredited to multiple Department of Defense (DoD) Impact Levels (ILs). It leverages a central configuration control authority to ensure consistent baseline management across all ILs. All models operate within this single environment, subject to its core physics and time services.

Digital Twin—A digital twin is a dynamic, virtual representation of a physical object, process, or system that mirrors its real-world counterpart in real time. Leveraging a digital ecosystem of sensors, networks and data, digital twins enable continuous monitoring, simulation, analysis, and prediction of performance regarding its real-world counterpart. They are used for optimization, maintenance, and to test, improve, and predict future outcomes before implementing changes in the physical world. Key aspects of a digital twin include near real-time optimization; digital twins use data from sensors to accurately reflect the current condition of the physical entity. Types of digital twins include digital representations of a single part of a system; virtual models of complete products; and complex operational processes.

Enterprise—An area of common activity and goals within an organization or between several organizations, where information and other resources are exchanged. (*The Common Approach to Federal Enterprise Architecture*, May 2012).

Governance—The exercise of authority, control, and shared decision making (planning, monitoring, and enforcement over the management of data assets. (DAMA DMBOK 2nd Edition)

Information—The meaning assigned to data by a known rule or set of rules. Generally, understanding concerning any objects such as facts, events, things, processes, or ideas, including concepts that, within a certain context and timeframe, have a particular meaning. The interpretation of data based on its context, including the: a) The business or mission meaning of data elements and related terms; b) The format in which the data is presented; c) The timeframe represented by the data; and d) The relevance of the data to a given usage. (DoD Office of the Chief Information

Officer Memorandum, *DoD Data Management Lexicon*, dated June 15, 2020, as derived from DAMA Dictionary of Data Management, 2nd Edition, 2017 and Hargrave's Communication Dictionary. IC CDOC Approved: Apr 2018).

Interoperability—The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (DoDI 8330.01).

Life Cycle—The sequence of stages that a particular unit of data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life.

Linked—Two or more items that are suggestively related.

MBSE—The formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later system life-cycle phases.

Metadata—Structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions (44 USC § 3502).

Mission Areas—A defined area of responsibility with functions and processes that contribute to mission accomplishment. (Definitions) The DoW Mission areas are the Warfighting Mission Area (WMA), Business Mission Area (BMA), DoW portion of Intelligence Mission Area (DIMA), and Enterprise Information Environment (EIE) Mission Area (EIEMA) (Ref: DoDD 8115.01).

Model—A model is a physical, mathematical, or logical representation of an actual or conceptual system, entity, phenomenon, or process. It is used to analyze, understand, or predict how the system performs under various conditions. (Defense Acquisition University Glossary).

Trusted—Users and applications can determine and assess the suitability of the source because the pedigree, security level, and access control level of each data asset or service is known and available (DoD Information Enterprise Architecture Version 2.0).

Understandable—Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs (DoD Information Enterprise Architecture Version 2.0).

Visible—The property of being discoverable. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset (DoD Information Enterprise Architecture Version 2.0).

Working Group—an interdisciplinary collaboration of people working on a specific topic, project or problem that would be difficult to develop under a traditional organizational structure or funding mechanisms. Cross-Functional Team makeup to develop products, report issues, and generate recommendations for associated Board to enable decisions and/or direction. Team construct consists of Subject Matter Experts (SMEs) comprised of contractor support, military and civilian personnel.

Attachment 2

MODEL STANDARDS AND FRAMEWORKS

A2.1. Model Standards and Frameworks. Model standards and frameworks are necessary to facilitate model sharing across the DoW, DAF, and USSF enterprises. Model standards and frameworks establish common and/or consistent practices for developing models. STARCOM organizations are to understand and use as appropriate the following reference artifacts when developing models and/or views:

A2.2. The DoD Architecture Framework (DoDAF). This framework provides structured viewpoints and models for system architects to describe architectures. The "Standards Viewpoint" is particularly relevant, articulating the applicable policies, business, technical, and industry standards for space systems and services.

A2.3. DoD M&S Standards. DoDI 5000.61 governs the VV&A for M&S used in testing and evaluation. While not space-specific, these standards apply to space-related simulations used for concept development and training.

A2.4. Space Force Doctrine: The Space Force establishes foundational principles and guidance for employing military space power. Space Doctrine Publications (SDPs) cover various topics, including sustainment (SDP 4-0) and planning (SDP 5-0), and emphasize interoperability with joint and allied forces.

A2.5. Defense Space Strategy: The DoD's 2020 strategy emphasizes ensuring stability in space, building military advantage, integrating space power into joint operations, and cooperating with allies and partners.

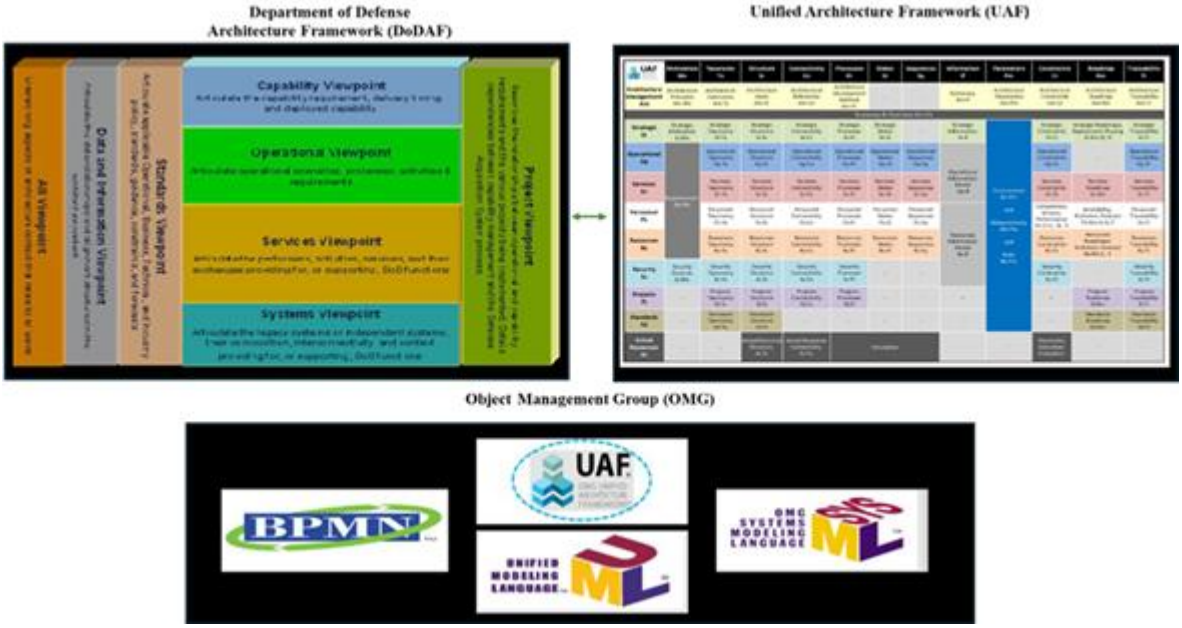
A2.6. DoD Directive 3100.10 Space Policy. Directs Commanders to baseline space capability needs and prioritized space-based mission needs and effects based on operational and contingency plans ensuring effective advocacy for space forces; and plan for employment of space capabilities within their areas of responsibility as well as integrate space capabilities and applications into training, exercises, war games, experiments, contingency plans, operational plans, military operations and security cooperation.

A2.7. Space Systems Acquisition Policy: To accelerate the acquisition of space capabilities, the Space Force has outlined tenets that prioritize speed, resilience, and integration. These include building smaller systems, leveraging commercial designs to minimize engineering, and using fixed-price contracts.

A2.8. Commercial Integration Strategy: The DoD’s 2024 Commercial Space Integration Strategy emphasizes adopting commercial standards and interfaces where appropriate to strengthen interoperability, speed, and resilience. This guides how the DoW integrates commercial space solutions into national security architectures.

A2.9. STARCOM Model Standard Taxonomy. STARCOM model development will include leveraging the DoDAF, Unified Architecture Framework (UAF), and Object Management Group (OMG) frameworks to meet the model intended form, fit and function.

Figure A2.1. STARCOM Model Standard Taxonomy.



A2.10. Department of Defense Architecture Framework (DoDAF). DoDAF is fundamentally about creating a coherent model of the enterprise to enable effective decision-making. DoDAF organizes the DoDAF-described Models into the following viewpoints:

A2.10.1. All Viewpoint are the overarching aspects of architecture context that relate to all viewpoints.

A2.10.2. The Capability Viewpoint the capability requirements, the delivery timing, and the deployed capability.

A2.10.3. The Data and Information Viewpoint capture data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.

A2.10.4. The Operational Viewpoint includes operational scenarios, activities, and requirements that support capabilities.

A2.10.5. The Project Viewpoint describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process.

A2.10.6. The Service Viewpoint is the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.

A2.10.7. The Standards Viewpoint articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems and services.

A2.10.8. The System Viewpoint, for Legacy support, is the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions.

A2.11. Object Management Group (OMG). OMG is responsible for several foundational standards that support object-oriented and model-driven software development and system design. Key standards that STARCOM will leverage include:

A2.11.1. Business Process Model and Notation (BPMN). A graphical notation standard for modeling business processes, providing a set of elements for representing process flows, including flow objects, connecting objects, artifacts, and swim lanes. BPMN is designed to be intuitive for business users and supports specification, analysis, and simulation of business processes.

A2.11.2. Systems Modeling Language (SysML). A graphical modeling language derived from the Unified Model Language (UML) and extended to support requirements, activities, constraints, and flows. SysML enables specification, analysis, and design of complex systems, including hardware, software, and processes. It is supported by organizations such as the International Council on Systems Engineering (INCOSE).

A2.11.3. Unified Model Language (UML). UML is a standardized, general-purpose graphical modeling language used to visualize, specify, document, and construct the artifacts of software-intensive systems. It employs diagrams including behavioral and structural diagrams and symbols to represent software architecture, design, and requirements in a clear, consistent way, facilitating communication and understanding among stakeholders.

A2.11.4. Unified Architecture Framework (UAF). UAF is the next generation of architecture frameworks, building on the legacy of the DoD Architecture Framework (DoDAF). UAF is used in the DoW as a standard for creating comprehensive enterprise architectures, building upon and succeeding DoDAF. UAF offers a model-based approach for defining and visualizing an organization's systems, processes, and strategy, supporting the creation of DoDAF-compliant views and facilitating collaboration across different stakeholders and organizations.

A2.11.4.1. UAF is based on the Unified Modeling Language (UML), Systems Modeling Language (SysML), the DoDAF, the U.K.'s Ministry of Defense's Architecture Framework. And the North Atlantic Treaty Organization's (NATO) Architecture Framework (NAF). Military and business requirements were combined to create the UAF and it serves both commercial and military interests.

A2.11.4.2. UAF specification consists of three main components. The Domain Metamodel (DMM) establishes the underlying foundational modeling constructs to be used in modeling an enterprise, as well as major entities within the enterprise. View specifications provide direction to the tool vendors and to those who are creating the architecture views regarding which DMM elements are pertinent to those views. The UAF Profile (UAFP) is an implementation of the DMM that specifies how the UAF views can be modeled using SysML notation.

A2.11.4.3. The UAF grid (Figure 4) has rows that represent typical stakeholder domains (or perspectives) that can be used when modeling an enterprise architecture. The grid has columns that represent the architecture aspects (in UAF these are called model kinds) that

correspond to the stakeholder domains. This grid is provided in the UAF standard as a structuring formalism for organizing the 71 view specifications defined within the UAF.

A2.12. DoDAF Architecture Framework V2.02.

A2.12.1. Model List. The DoDAF-described Models that are available in DoDAF V2.0 are listed in the **Table A2.1**. The list provides the possible models and is not prescriptive. The decision-maker and process owners will determine the DoDAF-described Models that are required for their purposes. The DoDAF-described Models are grouped into the following viewpoints:

A2.12.1.1. All Viewpoint (AV)

A2.12.1.2. Capability Viewpoint (CV)

A2.12.1.3. Data and Information Viewpoint (DIV)

A2.12.1.4. Operational Viewpoint (OV)

A2.12.1.5. Project Viewpoint (PV)

A2.12.1.6. Services Viewpoint (SvcV)

A2.12.1.7. Standard Viewpoint (StdV)

A2.12.1.8. Systems Viewpoint (SV)

Table A2.1. DoDAF V2.0 Models.

AV-1: Overview and Summary Information	Describes a Project's Visions, Goals, Objectives, Plans, Activities, Events, Conditions, Measures, Effects (Outcomes), and produced objects.
AV-2: Integrated Dictionary	An architectural data repository with definitions of all terms used throughout the architectural data and presentations.
CV-1: Vision	The overall vision for transformational endeavors, which provides a strategic context for the capabilities described and a high-level scope.
CV-2: Capability Taxonomy	A hierarchy of capabilities which specifies all the capabilities that are referenced throughout one or more Architectural Descriptions.
CV-3: Capability Phasing	The planned achievement of capability at different points in time or during specific periods of time. The CV-3 shows the capability phasing in terms of the activities, conditions, desired effects, rules complied with, resource consumption and production, and measures, without regard to the performer

	and location solutions.
CV-4: Capability Dependencies	The dependencies between planned capabilities and the definition of logical groupings of capabilities.
CV-5: Capability to Organizational	The fulfillment of capability requirements shows the planned capability deployment and interconnection for a particular Development Mapping Capability Phase. The CV-5 shows the planned solution for the phase in terms of performers and locations and their associated concepts.
CV-6: Capability to Operational Activities Mapping	A mapping between the capabilities required and the operational activities that those capabilities support.
CV-7: Capability to Services Mapping	A mapping between the capabilities and the services that these capabilities enable.
DIV-1: Conceptual Data Model	The required high-level data concepts and their relationships.
DIV-2: Logical Data Model	The documentation of the data requirements and structural business process (activity) rules. In DoDAF V1.5, this was the OV-7.
DIV-3: Physical Data Model	The physical implementation format of the Logical Data Model entities, e.g., message formats, file structures, physical schema. In DoDAF V1.5, this was the SV-11.
OV-1: High-Level Operational Concept Graphic	The high-level graphical/textual description of the operational concept.
OV-2: Operational Resource Flow Description	A description of the Resource Flows exchanged between operational activities.
OV-3: Operational Resource Flow Matrix	A description of the resources exchanged and the relevant attributes of the exchanges.
OV-4: Organizational Relationships Chart	The organizational context, role or other relationships among organizations.
OV-5a: Operational Activity Decomposition Tree	The capabilities and activities (operational activities) organized in a hierarchal structure.
OV-5b: Operational Activity Model	The context of capabilities and activities (operational activities) and their relationships among activities, inputs, and outputs; Additional data can show cost, performers, or other pertinent information.

OV-6a: Operational Rules Model	One of three models used to describe activity (operational activity). It identifies business rules that constrain operations.
OV-6b: State Transition Description	One of three models used to describe operational activity (activity). It identifies business process (activity) responses to events (usually, very short activities).
OV-6c: Event-Trace Description	One of three models used to describe activity (operational activity). It traces actions in a scenario or sequence of events.
PV-1: Project Portfolio	It describes the dependency relationships between the organizations and projects and the organizational structures needed to manage a portfolio of projects.
PV-2: Project Timelines	A timeline perspective on programs or projects, with key milestones and interdependencies.
PV-3: Project to Capability Mapping	A mapping of programs and projects to capabilities to show how specific projects and program elements help to achieve a capability.
SvcV-1 Services Context Description	The identification of services, service items, and their interconnections.
SvcV-2 Services Resource Flow Description	A description of Resource Flows exchanged between services.
SvcV-3a Systems-Services Matrix	The relationships among or between systems and services in a given Architectural Description.
SvcV-3b Services-Services Matrix	The relationships among services in a given Architectural Description. It can be designed to show relationships of interest, (e.g., service-type interfaces, planned vs. existing interfaces).
SvcV-4 Services Functionality Description	The functions performed by services and the service data flows among service functions (activities).
SvcV-5 Operational Activity to Services Traceability Matrix	A mapping of services (activities) back to operational activities (activities).
SvcV-6 Services Resource Flow Matrix	It provides details of service Resource Flow elements being exchanged between services

	and the attributes of that exchange.
SvcV-7 Services Measures Matrix	The measures (metrics) of Services Model elements for the appropriate time frame(s).
SvcV-8 Services Evolution Description	The planned incremental steps toward migrating a suite of services to a more efficient suite or toward evolving current services to a future implementation.
SvcV-9 Services Technology & Skills Forecast	The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future service development.
SvcV-10a Services Rules Model	One of three models used to describe service functionality. It identifies constraints that are imposed on systems functionality due to some aspects of system design or implementation.
SvcV-10b Services State Transition Description	One of three models used to describe service functionality. It identifies responses of services to events.
SvcV-10c Services Event-Trace Description	One of three models used to describe service functionality. It identifies service-specific refinements of critical sequences of events described in the Operational Viewpoint.
StdV-1 Standards Profile	The listing of standards that apply to solution elements.
StdV-2 Standards Forecast	The description of emerging standards and potential impact on current solution elements, within a set of time frames.
SV-1 Systems Interface Description	The identification of systems, system items, and their interconnections.
SV-2 Systems Resource Flow Description	A description of Resource Flows exchanged between systems.
SV-3 Systems-Systems Matrix	The relationships among systems in a given Architectural Description. It can be designed to show relationships of interest, (e.g., system-type interfaces, planned vs. existing interfaces).
SV-4 Systems Functionality Description	The functions (activities) performed by systems and the system data flows among system functions (activities).

SV-5a Operational Activity to Systems Function Traceability Matrix	A mapping of system functions (activities) back to operational activities (activities).
SV-5b Operational Activity to Systems Traceability Matrix	A mapping of systems back to capabilities or operational activities (activities).
SV-6 Systems Resource Flow Matrix	Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.
SV-7 Systems Measures Matrix	The measures (metrics) of Systems Model elements for the appropriate timeframe(s).
SV-8 Systems Evolution Description	The planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.
SV-9 Systems Technology & Skills Forecast	The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future system development.
SV-10a Systems Rules Model	One of three models used to describe system functionality. It identifies constraints that are imposed on systems functionality due to some aspect of system design or implementation.
SV-10b Systems State Transition Description	One of three models used to describe system functionality. It identifies responses of systems to events.
SV-10c Systems Event-Trace Description	One of three models used to describe system functionality. It identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.

Attachment 3

MODEL LIFECYCLE MANAGEMENT

A3.1. Model Development. Digital model development enhances capability and/or system design prior to and post system testing and fielding; improves the Warfighter training experience; and reveals potential strategic and operational strategies and shortfalls. Digital model development includes defining the model requirements and objectives, building the model, incorporating validated authoritative data, performing Digital Engineering (DE), VV&A, and actively sustaining the model until decommissioning.

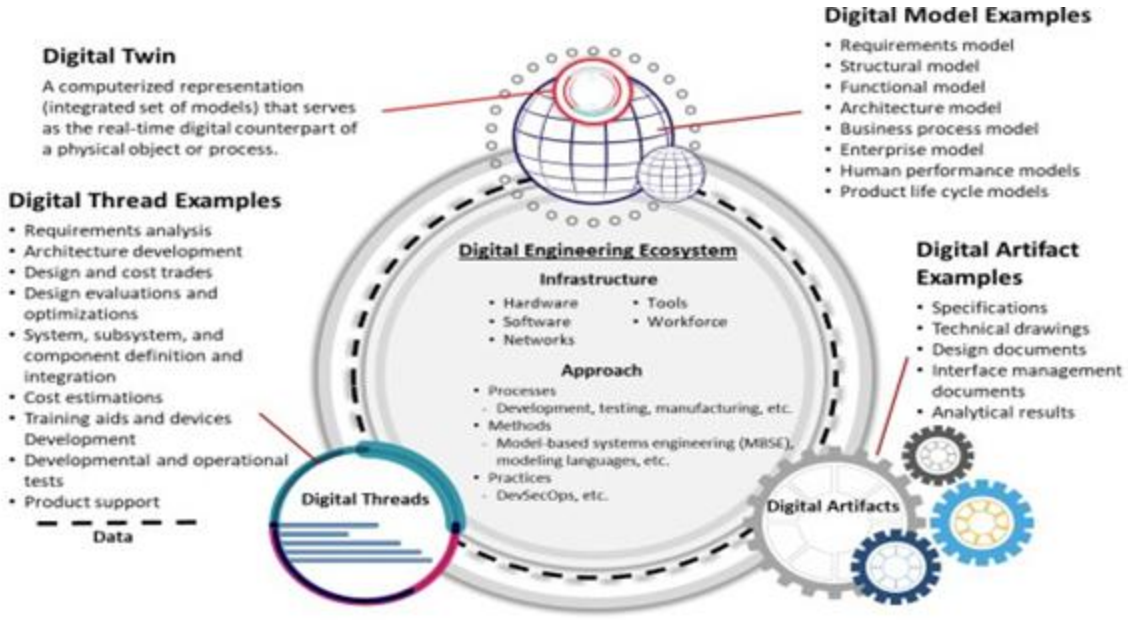
A3.2. Digital Engineering Framework. The DoW is transforming its engineering practices to incorporate digital technology and innovations into an integrated, digital, model-based approach. The DoW uses digital engineering methodologies, technologies, and practices across the life cycle of defense acquisition programs, systems, and systems of systems to support research, engineering, and management activities as outlined in DoDI 5000.97, *Digital Engineering*.

A3.2.1. Digital engineering must be addressed in the acquisition strategy, including how and when digital engineering will be used across system life cycle and expected benefits of its use. In addition, as specified in DoDI 5000.88, *Engineering of Defense Systems*, certain initiatives must include a digital engineering implementation plan in the systems engineering plan.

A3.2.2. Digital engineering requires planning and providing resources for digital methods (e.g., model-based systems engineering (MBSE), product life-cycle management, computer aided design) in support of modeling activities.

A3.2.3. Models developed after 21 December 2023 will incorporate digital engineering for the capability in development unless the decision authority provides an exception. Models developed before 21 December 2023 may incorporate digital engineering when it is practical, beneficial, and affordable, but are not required to do so.

Figure A3.1. Digital Engineering Framework.



A3.3. VV&A Framework. Ensure digital models, simulations, and associated data are verified, validated, and accredited for their intended use, in accordance with Air Force Instruction 16-1001, *Verification, Validation and Accreditation (VV&A):*

A3.3.1. M&S requirements are developed as part of various activities (operational test, life cycle management, decision-making, training, etc.) and may have varying levels of VV&A associated with the development and define the use of models for specific purposes.

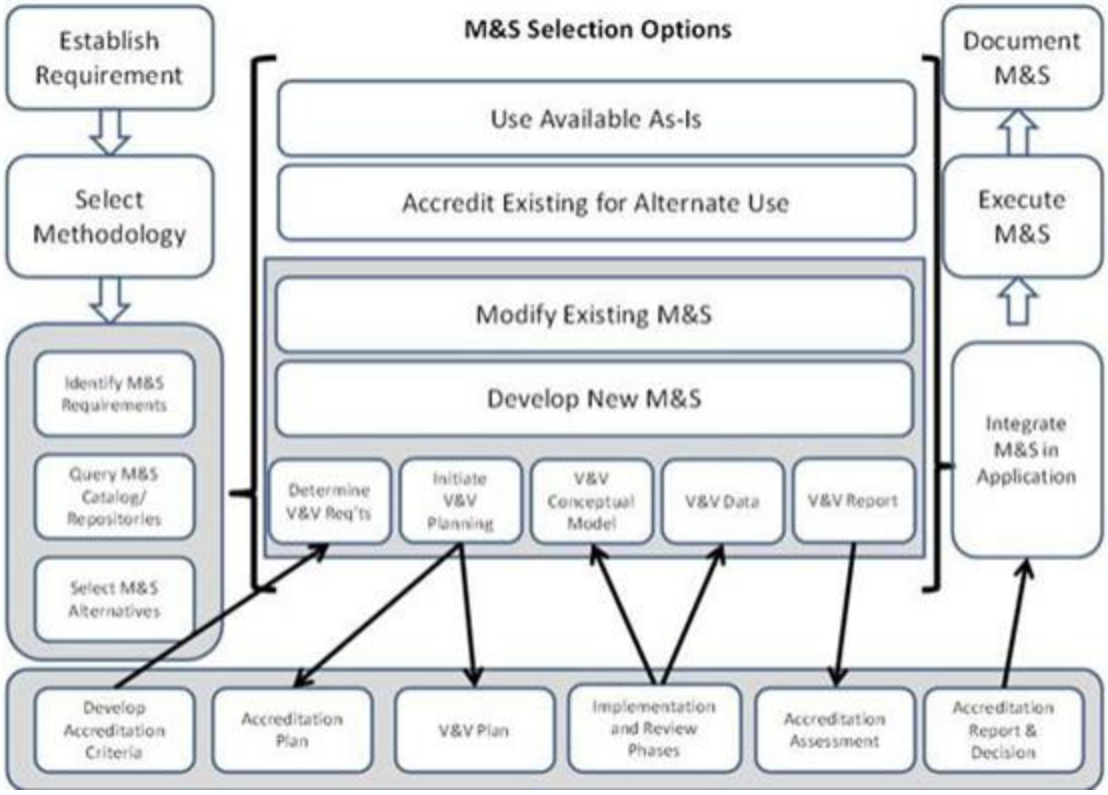
A3.3.2. Verification identifies and eliminates mistakes in logic, mathematics, or programming to ensure that a system element meets design-to or build-to specifications. This process establishes whether the M&S code and logic correctly perform the intended functions. Further, it establishes to what extent M&S development activities conform to state-of-the-practice software engineering techniques.

A3.3.3. The validation process evaluates the effectiveness and suitability of the M&S application’s conceptual model. It has two main components: structural validation, which includes an internal examination of M&S assumptions, architecture, and algorithms in the context of the intended use; and output validation, which determines how well the M&S results compare with the perceived "real world."

A3.3.4. The accreditation determination considers the Verification and Validation (V&V) status of a specific model version, its data support (source, quality, and verification), and the analysts or users that operate the model and interpret its results. The accreditation authority is the individual who is responsible and accountable for decisions or actions based upon the specific M&S usage. The decision to accredit a model or simulation rests solely with the accreditation authority. The accreditation authority determines the level of effort needed to support the accreditation decision, whether it consists of conducting additional V&V activities or simply reviewing the existing M&S documentation and past VV&A history. Accreditation is management responsibility of the requiring agency, assisted by the designated V&V agent.

A3.3.5. VV&A Process.

Figure A3.2. VV&A Process.



A3.3.6. VV&A Documents. MIL-STD-3022, *Documentation of Verification, Validation, and Accreditation (VV&A) for Model and Simulations,* standard establishes templates for the four core products of the M&S, and VV&A processes: Accreditation Plan; V&V Plan; V&V Report, and Accreditation Report. These documents are normally prepared and used at different times and by different groups, much of the information included in each is common and should be shared. The templates provide a common framework and interfacing capability between the four documents and support consistency and efficiency. Additionally, the plans and reports produced by following the templates serve as a communications device between the participants in the VV&A processes.

Figure A3.3. VV&A Documentation.

Accreditation Plan	V&V Plan	V&V Report	Accreditation Report
Executive Summary	Executive Summary	Executive Summary	Executive Summary
1 Problem Statement	*1 Problem Statement*	*1 Problem Statement*	*1 Problem Statement*
2 M&S Requirements and Acceptability Criteria	*2 M&S Requirements and Acceptability Criteria*	*2 M&S Requirements and Acceptability Criteria*	*2 M&S Requirements and Acceptability Criteria*
3 M&S Assumptions, Capabilities, Limitations & Risks/Impacts	*3 M&S Assumptions, Capabilities, Limitations & Risks/Impacts*	*3 M&S Assumptions, Capabilities, Limitations & Risks/Impacts*	*3 M&S Assumptions, Capabilities, Limitations & Risks/Impacts*
4 Accreditation Methodology	4 V&V Methodology	4 V&V Task Analysis	4 Accreditation Assessment
5 Accreditation Issues	5 V&V Issues	5 V&V Recommendations	5 Accreditation Recommendations
6 Key Participants	*6 Key Participants*	*6 Key Participants*	*6 Key Participants*
7 Planned Accreditation Resources	7 Planned V&V Resources	7 Actual V&V Resources Expended	7 Actual Accreditation Resources Expended
		8 V&V Lessons Learned	8 Accreditation Lessons Learned
Suggested Appendices *A M&S Description* *B M&S Requirements Traceability Matrix* *C Basis of Comparison* *D References* *E Acronyms* *F Glossary* G Accreditation Programmatics H Distribution List	Suggested Appendices *A M&S Description* *B M&S Requirements Traceability Matrix* *C Basis of Comparison* *D References* *E Acronyms* *F Glossary* G V&V Programmatics H Distribution List I Accreditation Plan	Suggested Appendices *A M&S Description* *B M&S Requirements Traceability Matrix* *C Basis of Comparison* *D References* *E Acronyms* *F Glossary* G V&V Programmatics H Distribution List I V&V Plan J Test Information	Suggested Appendices *A M&S Description* *B M&S Requirements Traceability Matrix* *C Basis of Comparison* *D References* *E Acronyms* *F Glossary* G Accreditation Programmatics H Distribution List I Accreditation Plan J V&V Report

A3.3.6.1. The purpose of this standard is to provide a common framework for sharing information throughout the VV&A processes. The common method of documentation benefits participants in the VV&A processes by eliminating unnecessary redundancy and facilitating reuse of information when accrediting an M&S for the intended use.

A3.3.7. Management of digital models shall be fully woven into the model lifecycle processes. VV&A Planning: for every new AI model and/or DT, a formal VV&A Plan shall be developed (per MIL-STD-3022 guidelines) just as with any other simulation model. The plan will identify the model's intended use, required fidelity, and an uncertainty budget for that use, and will specify validation methods (e.g., test scenarios, comparison against real data) and acceptance criteria. Golden scenarios should be designated in the VV&A plan, e.g., canonical test cases drawn from real-world events or key use-cases that serve as benchmark tests for the model. For instance, a known jamming incident might be a golden scenario for evaluating an AI-driven electronic warfare model.

A3.3.8. Digital Critical Design Review (CDR). The system DT or high-fidelity digital model of the system shall successfully execute a Government-witnessed and approved test plan within the S-DR. The model must demonstrate required performance within established validation criteria against mission-relevant scenarios. The VV&A Authority is responsible for providing the Government-approved test plan and validation criteria for this gate. Successful completion of this activity is a mandatory prerequisite for the program to receive approval to proceed past CDR, formally enforcing the command's "test before you invest" paradigm.

A3.3.9. Operational Effectiveness and Suitability. For any model intended for use by an operator or in direct support of TT&E events, the VV&A process must include an assessment

of its operational effectiveness and suitability. This assessment shall be conducted through formal user-in-the-loop testing with designated operational personnel (i.e., warfighters). The final V&V Report must document the findings, confirming that the model is effective, suitable, and trusted by its intended users for the specified mission context. This finding is a prerequisite for a final accreditation decision.

A3.4. Sustainment. Model management is treated as a life-cycle activity, fully integrated with system sustainment. Sustain the S-DR and its models as enduring assets, updating them as the system evolves to prevent divergence. Near-real-time updates keep the DTs synchronized with the fielded system provides update mechanisms. After any significant event or on a regular schedule, new operational data (telemetry, performance metrics, etc.) will flow into the S-DR to recalibrate and refine models. If the physical system's configuration changes (hardware or software updates), it's DT is updated in parallel. This continuous synchronization ensures the DT remains an effective proxy for the real system. The Product Support Strategy incorporates DT sustainment, leveraging authoritative models and data to inform maintenance and upgrades. To support this, key deliverables include a DT Description (DTD) capturing each model's design, assumptions, and support requirements, and a SBOM and/or HBOM for the S-DR to ensure transparency and cybersecurity. These artifacts are provided to the government by the developer to full insight and technical data needed to independently operate and update the DT over the system's life. Where beneficial, also consider adopting existing proven models from industry or other DoW organizations; an "adopt-and-wrap" approach will be used to integrate such models under our standards and VV&A regime.

A3.4.1. In accordance with Department of Defense Instruction 5000.97 *Digital Engineering:* Identify and maintain model-centric baselines, approaches, and applications in a digital form that integrates the technical data and associated digital artifacts that stakeholders generate throughout the system lifecycle. Digital model(s) will use and/or align to DoW and/or industry-driven model standards and best practice models, methods, and underlying data structures to maximize interoperability. Digital models shall undergo periodic revalidation against current data that has been randomly sampled to detect performance drift. Performance drift is the gradual or sudden decline in a machine learning model's accuracy and reliability over time after deployment, caused by real-world changes in data patterns or relationships that differ from its training data, leading to faulty predictions and making the model obsolete. To prevent regression, newly deployed digital models must demonstrate accuracy equivalent to that of previously deployed models. Re-validation must include data used to test prior model versions, in addition to data specific to the latest version, to ensure drift is not present. If output/s exceed the accredited uncertainty budget, the model owner shall retrain and/or recalibrate or remove from use pending VV&A review. Significant changes (algorithms, training data, or environment inputs) create a new version requiring VV&A reassessment prior to use.

A3.4.2. Establish a standard approach for developing each type of digital model. Use existing modeling standards and approaches to improve integration of models across the DoW. Evaluate all digital models to ensure they are accurate, complete, trusted, and reusable. Develop digital models in accordance with applicable DoW policies, guidance, and standards. Reference the Acquisition Streamlining and Standardization Information System (ASSIST) (available at **https://assist.dla.mil/online/start**) and DoW Information Technology Standards Registry repositories as government-adopted authoritative sources of truth for standards.

A3.4.3. Develop and implement plans to establish current, consistent, enduring, and authoritative sources of truth for digital models and data. Reference the 2020 DoD Data Strategy for additional information on mandated data attributes, including achieving visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS) goals.

A3.4.4. Drift Monitoring. Perform periodic drift checks for DT/AI models as part of their established maintenance cycle, to validate model performance against current data and detect performance drift. Owners of AI models shall implement a plan to monitor model performance over time (especially during operational use) to detect model drift. *Drift* refers to a model's degradation as real-world conditions change beyond what it was trained on. Procedures shall include periodic re-validation of AI models against new data to check for drift. If a model's outputs begin to deviate significantly from expected real-world results (e.g., a debris collision risk model under-predicts events compared to newly observed data), it triggers maintenance actions: retraining, recalibration, or if necessary, retirement of the model.

A3.4.5. Rollback and Fail-Safe. Any AI model deployed in training or testing must have a defined rollback procedure to quickly revert to a previous trusted model (or a safe default state) if the AI behaves unexpectedly or unsafely. The VV&A Authority shall approve a Model Rollback Plan for each operational AI model, specifying how to detect unsafe or anomalous outputs and immediately remove or replace the model. For example, if an AI agent starts providing implausible or dangerous tactics in a simulation, operators must have clear instructions to suspend that model and fall back to a proven scenario or manual control. Rollback capability ensures that AI failures do not compromise mission training, much like version control for software, the previous stable model version is kept available and can be restored on short notice. *(The importance of an incident response and rollback plan for models has been highlighted in STARCOM's implementation roadmap.)*

A3.4.5.1. Rollback on Anomaly. If a model exhibits a significant anomaly while being used for any TT&E event or in direct support of an operational mission, the operator shall execute the approved Model Rollback Plan. This plan must, at a minimum, direct the operator to: (1) immediately cease use of the anomalous model and revert to the last accredited version or a pre-defined safe state; (2) isolate and preserve all data related to the anomalous event for post-event analysis; and (3) promptly notify the model's governing authority and the VV&A Authority of the incident. The incident and all subsequent actions shall be formally logged for VV&A review.

A3.4.6. Retention of Baselines and Data. In accordance with model retention, the "last approved" configuration of each DT/AI model and S-DR must be retained. When an update occurs, the superseded version (and its underlying training data or configuration snapshot) shall be archived rather than overwritten, enabling rollback if needed and providing a historical record of the model's evolution. The S-DR will maintain baseline snapshots at major version milestones; those snapshots (including scenario data, input databases, etc.) are kept permitting reconstruction of past exercises or analyses. Similarly, any data used to train or validate AI models (training datasets, test scenario outputs) is considered part of the model's VV&A evidence and shall be retained for the life of the model (per records management policy). This allows STARCOM to answer future questions such as "how was this model trained or tested?" even if personnel have changed. All documentation and record-keeping for VV&A of AI/DT models shall align with MIL-STD-3022 (which provides standard templates for VV&A plans, reports, etc.). Include any AI-specific VV&A artifacts (for example, an AI model training data

report or a drift assessment report) as new record types. By integrating these requirements into the lifecycle STARCOM ensures DT/AI models are not managed ad hoc, but with the same rigor as any model-of-record used for operations.

A3.4.7. Continuous Performance Monitoring and AI Risk Controls. Managing AI models is not a "one and done" activity. Models will have ongoing monitoring to detect model performance drift and manage AI-specific risks. S-DR will capture operational performance data for each model and compare it to expectations; if drift is detected (i.e. the model's accuracy or behavior deviates beyond acceptable bounds due to changing real-world conditions or unanticipated scenarios), it will trigger an investigation and model update cycle. Define clear thresholds and triggers for model performance (e.g., error rates, confidence levels) that, if exceeded, prompt re-calibration, retraining, or fallback to a safe mode. In addition, rollback procedures are in place: if a newly deployed model exhibits anomalous or unsafe behavior, the system can swiftly revert to the last trusted model version. S-DR maintains a library of validated model versions, enabling rapid rollback if needed to ensure continuity of operations and safety. These controls, along with rigorous testing, implement a conservative "trust but verify" approach to AI deployment. They align with emerging DoW AI test guidance calling for documented model performance and readiness to intervene if AI behavior diverges from expected norms.

A3.4.8. Retention and Decommissioning.

A3.4.8.1. Retention. Retention includes raw training data, cataloging and/or labeling records; and training configuration files (including but not limited to model hyperparameters). Models shall be retained based on their operational, historical, or analytical value, as outlined in the STARCOM Model Retention Schedule:

A3.4.8.1.1. Last known good retention. Retain the last accredited digital model version and its associated data and/or configuration snapshot to support rollback, audit, and reproducibility.

A3.4.8.1.2. Mission Training Model. Retained for a minimum of 7 years or until superseded by new scenarios or doctrine.

A3.4.8.1.3. Training Model Sources. Retained for the life of the model plus 5 years for auditability, retraining, and revalidation purposes.

A3.4.8.1.4. Test and Evaluation Model. Retained for 7 years or as required by test certification standards.

A3.4.8.1.5. Baselines. Retain at a minimum the last three previous stable versions of each digital model (including training and evaluation datasets and configuration snapshots) to support rollback, provenance, and future audits. Superseded versions shall be cataloged and archived, not overwritten, and remain discoverable in the catalog and archived, not overwritten, and remain discoverable in the catalog with validity dates.

A3.4.8.2. Decommissioning.

A3.4.8.2.1. Secure Decommissioning. STARCOM must incorporate retention and deletion schedules, especially for models leveraging classified or AI-sensitive content.

AI-sensitive content includes personal, confidential, or potentially harmful content if misused and/or exposed (e.g., medical records, or PII).

A3.4.8.2.2. Suspension and/or Decommissioning. Legal advice shall be required by the STARCOM Judge Advocate (JA) if a digital model and/or its associated data becomes subject to an investigation.

Attachment 4

MODEL SHARING AGREEMENT TEMPLATE

Figure A4.1. Model Sharing Agreement Template.

Space Training and Readiness Command (STARCOM)

Model Sharing Agreement

[Date][Version Number]

[***Note: This template provides an example for a memorandum of agreement between two organizations who would like to engage in a shared confidentiality relationship in order to facilitate the exchange of a model/s from external agencies. Organizations should feel free to adapt and customize this agreement as appropriate. Include all model sharing information points outlined in paragraph 1.2.7.1 of this Instruction***]

1. NAME OF ORGANIZATIONS ENTERING INTO AGREEMENT

Organization 1
Name of Organization Requestion Data:
Address:
Phone:

Organization 2
Name of Organization Providing Data:
Address:
Phone:

2. LEGAL AUTHORITY AND REASONS OF THE AGREEEMENT

In this section, both organizations should state in non-technical language the purpose(s) for which they are entering into the agreement. For example, models will be shared between organizations to facilitate... (add specific details here).

3. RESPONSIBILITIES AND OBLIGATIONS OF THE AGREEEMENT

In this section, both organizations should state in non-technical language their responsibilities and obligations of the agreement, including third-parties rights and responsibilities.

4. MODEL/S TO BE SHARED AND SUPPLEMENTAL INFORMATION

In this section, capture in non-technical language the model/s to be shared and associated supplemental information. When sharing an AI model or DT, the Provider shall include the model's VV&A documentation (accreditation memo and model card) and a Software/Hardware Bill of Materials (SBOM/HBOM) for transparency. The Receiving organization agrees to employ the model only within its accredited intended use (unless re-accredited) and to notify the Provider and STARCOM VV&A Authority of any anomalous or unsafe behavior. A rollback plan (reversion to a prior trusted version or removal of the model) shall be in place and executable on request of the providing authority if an incident occurs.

5. METHOD OF MODEL SHARING

In this section, capture in non-technical language the method in which model/s will be shared, must include details about the supplying and receiving system/s or data platform/s.

6. DATA EXCHANGE, UPDATE, AND/OR BACKUP FREQUENCY

In this section, capture in non-technical language the frequency at which model/s will exchanged, and/or updated.

7. MODEL SUPPLIER AND MODEL REQUESTOR ACTIVITIES

In this section, both organizations capture in non-technical language their access to information and decision right following any exchange.

8. MODEL SECURITY

In this section, capture in non-technical language the security and access control requirements for the model exchange and receipt, including how access will be audited for the record.

9. MODEL INCIDENT REPORTING

In this section, capture in non-technical language how both organizations will accomplish timely reporting of incidents affecting model/s covered by the agreement.

10. RESOURCE IMPACT

In this section, both organizations should state in non-technical language the resource impacts for implementing the model sharing agreement.

11. RISK MITIGATION AND DISPUTE RESOLUTION

In this section, both organizations should state in non-technical language risk and dispute mitigation methodologies.

12. AGREEMENT TERMINATION OR TRANSFER

In this section, both organizations should state in non-technical language the terms for this agreement to be terminated or transferred, and any notice period that will be required.

13. PERIOD OF AGREEEMENT

The period of agreement shall extend from _____to

_____.

14. CONFIDENTIALITY

In this section, the organizations should describe the technical and physical safeguards they will implement to protect the confidentiality of the model shared and prevent unauthorized access. This includes limiting access to individuals with a need-to-know, storing electronic protected and/or encrypted computers and tablets, etc. Organizations may also want to include a copy of the confidentiality agreement that all staff using the model will be required to sign prior to the start of the model sharing agreement.

15. SIGNATURES

_____

Signature Block of Organization Requesting Model

_____

Signature Block of Organization Providing Model

Attachment 5

MODEL FIDELITY, CREDIBILITY AND RISK MANAGEMENT

A5.1. Fidelity Bands. Defining and managing model fidelity levels in S-DR.

A5.1.1. Define Discrete Fidelity Levels. Establish clear fidelity "bands" (e.g., High, Medium, Low) for models in the S-DR. Each band corresponds to a defined level of detail, resolution, and uncertainty tolerance appropriate to different use cases. For example, a high-fidelity band might capture high-resolution physics or full orbital mechanics suitable for detailed engineering analysis, whereas a medium-fidelity band might use simplified models adequate for real-time training or mission rehearsal. This categorization ensures stakeholders understand the reliability and limitations of a model's results based on its fidelity level. (DTs may vary in fidelity based on the use case, so matching fidelity to context is essential.)

A5.1.2. Validation Requirements per Band. Validation and V&V criteria will be tailored to each fidelity band. Higher-fidelity models must meet stringent validation benchmarks (e.g., error margins within X% against real-world data, verified physics-based accuracy) before acceptance. Lower-fidelity models can have more relaxed validation criteria but must be accredited as fit for their intended purpose (e.g., qualitative training scenarios). Each band's acceptable error ranges, test cases, and VV&A requirements are documented. For instance, a high-fidelity thermal model may need thermal vacuum test correlation, whereas a low-fidelity training model might be validated by demonstrating representative behavior in key scenarios. By scaling VV&A rigor to fidelity, avoid over- or under-testing models.

A5.1.3. Controlled Transitions and Usage Limits. The use of a given fidelity model is restricted to appropriate applications, and transitions between fidelity levels are deliberate. If an analysis or exercise requires greater detail, the team will move to a higher-fidelity model (with associated higher computational cost) rather than stretching a lower-fidelity model beyond its valid scope. Conversely, for fast-running evaluations, a lower-fidelity model may be substituted if validated as adequate. Any known limitations of lower-fidelity representations (e.g., "Medium fidelity Guidance model not valid above 60° angle of attack") are clearly documented and communicated to users. This prevents misapplication of models. If results from a lower-fidelity model drive decisions, risk mitigations (e.g., follow-up runs with a high-fidelity model) are employed to confirm critical outcomes. In summary, fidelity bands are managed to ensure the model's fidelity always matches the decision at hand, balancing speed and accuracy.

A5.2. Near-Real-Time Updates. Keeping the DT synchronized with the operational system.

A5.2.1. Automated Telemetry Ingestion: Implement automated data pipelines from the fielded system into the S-DR to enable near-real-time model updates. Key system telemetry, mission data, and configuration changes are uploaded at regular intervals (e.g., immediately post-mission or in daily batches) to refresh the DT's state. This could include sensor readings, health and status logs, software updates, etc. Tools will parse and ingest data in standardized formats to update corresponding model parameters or to initialize simulations. Automated ingestion minimizes lag and human error in keeping the DT current.

A5.2.2. Update Frequency Driven by Need. The latency of updates is tailored to operational needs. For critical systems or AI models whose validity depends on environmental data,

updates might be virtually continuous or within hours (near-real-time), ensuring the DT never grows stale. For slower-evolving aspects, a periodic (e.g., weekly or monthly) update may suffice. These cycles are defined in the Data Management Plan. The guiding rule is that significant changes and/or events in the real system is reflected in the DT for long. If true real-time streaming of certain data is feasible and valuable (e.g., live state vectors during an exercise), the architecture will accommodate it. Otherwise, timely batch updates are scheduled to maintain synchronization. (A DT should remain synchronized with its physical counterpart to be useful).

A5.2.3. Reflect Configuration Changes Promptly. Whenever a configuration change occurs on the real system, such as a firmware update, hardware replacement, or updated external environment (new threat parameter, new orbital data), the same change is applied to the S-DR's data and models. The configuration management process includes triggers to update the DT whenever an engineering change is implemented. This ensures the DT's baseline never drifts from the actual system configuration. The DTD and model registry are updated to record the new configuration, and a validation test (e.g., regression simulation) may be run to verify that the DT with the new change still behaves as expected.

A5.2.4. Data Quality Checks. Each ingestion and update will include data validation checks. Poor or anomalous data (corrupted files, out-of-range values) are flagged and reviewed by engineers before being committed to the DT. This prevents "garbage in, garbage out" issues that could degrade the DT's accuracy. The S-DR team also monitors for significant deltas between expected and actual data (e.g., if the real system performance differs notably from the DT's prediction), such deltas might indicate model drift or an emerging issue, prompting analysis. The update mechanism thus not only keeps the DT current but also serves as a diagnostic tool to compare DT vs. real performance continuously.

A5.3. System DT Sync Triggers. Events and conditions that initiate synchronization between the live system and its DT.

A5.3.1. Scheduled Sync Intervals. Establish regular sync intervals as a baseline, for example, a nightly data sync or weekly comprehensive update. These scheduled syncs ensure even in absence of specific triggers, the DT is periodically refreshed. The schedule is aligned with operational tempo (e.g., daily during on-orbit operations, less frequently during dormancy). A scheduled sync typically pulls the latest telemetry, maintenance actions, and configuration changes into S-DR, and pushes any DT-derived insights needed for upcoming operations.

A5.3.2. Post-Event Triggers. Any major event will trigger an immediate synchronization cycle. Major events include flight tests, training exercises, operational missions, anomalies/failures, or any occurrence where the system experienced conditions outside normal parameters. After such events, the DT is updated with high-fidelity event data (e.g., trajectory logs, sensor recordings) to capture what happened. Then the DT runs simulations replicating the event to compare predicted vs actual outcomes. This post-event sync allows the team to calibrate models based on reality, for instance, if a satellite maneuver had a slightly different outcome than predicted, the DT's orbital model can be adjusted. Anomalies are of particular importance: if the system encounters unexpected behavior, the DT is synced and used to investigate root causes in a controlled setting.

A5.3.3. Pre-Mission and/or Pre-Test Configuration Check. Before significant operations (a major deployment, a crew training event, a large-scale exercise), a pre-event sync is conducted.

This ensures the DT is fully up to date with the latest system status and environmental data prior to using it for mission rehearsal or test predictions. For example, before a wargame exercise, the DT might be synced with current orbital conjunction data, recent sensor calibration constants, etc., so that the virtual scenario starts from an accurate state. This trigger is essentially a readiness check: the DT is synchronized and validated as reflecting the real system, so that any "rehearsal" or analysis in the DT will be relevant.

A5.3.4. Change-driven Updates. Synchronization is triggered whenever there is a configuration change or update to the system or its software. This includes installation of a new AI model on the operational system, changes to algorithms, updated space threat library data, or any modification that could cause the DT and system to diverge. Upon such a change, engineers will input the change into the DT (e.g., load the new AI model into the S-DR, update the parameters or software version in the simulation) and run a validation test in the DT environment. Only after the DT demonstrates acceptable performance with the change (per VV&A) will the change be considered fully verified. This mechanism effectively uses the DT to regression-test all significant updates.

A5.3.5. Performance Drift or Anomaly Detection. The system and DT are continuously compared for consistency. If monitors detect that the DT's predictions are trending away from actual system performance (e.g., fuel usage, processing time, accuracy metrics differ beyond a set threshold), a trigger is activated to resynchronize and investigate. Such drift triggers prompt an unscheduled sync: pulling recent data, updating models (or model parameters), and running diagnostics in the DT to identify whether the model has grown inaccurate (requiring retraining or fixing) or the system behavior changed (e.g., hardware aging). By addressing drifts promptly, maintain alignment between expectation and reality. As Aerospace's DT guidance suggests, a faithfully maintained DT reduces lifecycle surprises, these triggers are designed to keep the DT faithful and surprises at bay.

A5.4. Robustness Testing. Stress-testing AI models within the DT to ensure reliability under all conditions.

A5.4.1. Extensive Scenario Simulation ("Test to Fail"): For each AI model, conduct a "Digital Cousin" robustness campaign (defined as the execution of the same core model across a large set of runs where environmental or system parameters are deliberately varied to test design resilience), which includes Monte Carlo and edge-case simulations. Monte Carlo and edge-case simulations in the S-DR to probe model behavior under a wide range of conditions, including extreme and unlikely scenarios. Thousands of runs will be executed varying environmental conditions, initial states, failure modes, and random perturbations to observe how the model performs. The goal is to find the model's breaking points and corner cases before deployment. For example, a guidance AI would be tested with highly off-nominal sensor inputs, worst-case timing delays, and simultaneous subsystem failures. Any scenario that causes the model to misbehave or degrade significantly is flagged for mitigation (either retraining the model on that scenario, implementing a safeguard, or explicitly constraining the model's use). By testing to failure in simulation, we ensure the operational system is less likely to encounter a surprise the model can't handle.

A5.4.2. Adversarial and Constructive Stressors. The S-DR will incorporate constructive adversarial testing, using simulated actors and generative techniques to challenge the model. For instance, AI-driven "red team" agents can be introduced in the simulation to mimic

intelligent adversaries or off-script behaviors (e.g., an enemy satellite that maneuvers unpredictably or a swarm of debris causing sensor confusion). We will also use techniques like adversarial perturbations on inputs to test AI robustness (e.g., slightly altering imagery to see if a perception model is fooled). The DT environment permits mixing real-world replay with hypothetical variations, so we will take real events (telemetry logs, scenarios) and alter variables to create new test cases. Tools in S-DR can generate synthetic sensor data or environmental conditions not yet seen in reality, pushing models into novel regimes. The use of generative simulation (e.g., varying lighting, creating synthetic sensor feeds) helps ensure models are not brittle and can generalize.

A5.4.3. Performance Metrics and "Prove-It" Criteria. Quantitative metrics are tracked during robustness testing, e.g., success rate, accuracy, false alarm rate, resource usage, across all the scenario variations. Set exit criteria that define what it means for a model to be "good enough" under stress. For example, "the AI must maintain control >99% of the time in 10,000 Monte Carlo runs" or "no single failure causes more than 10% performance degradation." If a model fails to meet a criterion, it is not deployed; design or training must be improved. We enforce the mantra "prove it in the DT, then deploy": only models that have conclusively demonstrated required performance and reliability in the DT will be authorized for operational use. Additionally, we perform regression testing, if a model is updated, it must again prove it meets all robustness criteria in DT tests before it replaces the old version. These practices mirror best-in-class AI assurance approaches and DoW test community expectations for AI (e.g., ensuring robust AI-enabled performance through updates and new missions). Ultimately, by the time an AI model goes live, it has already faced and overcome a gauntlet of worst-case scenarios in the DT, giving high confidence in its resilience.

A5.4.4. Human Oversight and Human-Systems Interaction (HSI) Factors. Robustness testing isn't limited to the model in isolation; we also examine how the AI interacts with human operators and other system elements. The DT environment allows incorporation of operator-in-the-loop tests to see how humans respond to AI outputs under stress (e.g., does the crew get overloaded with false alarms during edge cases?). Any HSI issues identified (such as unclear AI decision rationale leading to human error) result in either model interface adjustments or training mitigations. Likewise, if the AI's actions could induce unsafe system states, we identify whether safeguards or "operational guardrails" are needed. All these aspects are evaluated in simulation so that, in real operations, both the AI and the human team are prepared for tough situations.

A5.5. Adopt-and-Wrap. Incorporating external models by adoption and interface wrapping.

A5.6. Adopt Proven Models When Feasible. Seek to reuse or integrate existing models (from government libraries, academia, industry) to avoid reinventing the wheel, provided they meet our needs. When an external model or component is adopted ("as-is" intellectual content), it will be "wrapped" with a software/interface layer that adapts it into the S-DR. This wrapper handles differences in data formats, units, runtime interfaces, and ensures the external model can plug into our architecture seamlessly. The wrap may include translation of I/O, invocation of the model within our simulation framework, and any shims needed for compatibility with S-DR's standards (see Section 5). For example, if adopting a commercial physics engine, a wrapper will feed it S-DR's scenario data formats and extract results back into our databases. Wrapping allows leverage cutting-edge external tech while maintaining a consistent environment.

A5.7. Apply VV&A and Control Measures. Adopted models are not exempt from our VV&A process. Each third-party or Government off the Shelf (GOTS) model goes through the same verification and validation rigor as internally developed models before being trusted in the S-DR. The wrapper often facilitates this by providing hooks for monitoring and sandboxing the adopted model. For instance, the wrapper can enforce runtime limits, sanity-check the model's outputs against expected ranges, and log its performance for review. If the adopted model begins to behave unexpectedly (e.g., producing non-physical outputs), the wrapper can trigger a failsafe, such as reverting to a simpler backup model or alerting an operator, thereby mitigating risks from black-box components. The result is that even if we don't have full insight into an adopted model's inner workings, we contain it within a controlled interface that maintains system integrity. All assumptions or limitations coming with the external model (from its documentation or known usage constraints) are captured in its metadata record (model card) and respected in operation.

A5.8. Licensing, Intellectual Property, and Transparency. When adopting a model, ensure it has sufficient rights and documentation to use and sustain that model long-term. Data rights considerations (per DoDI 5000.82/5000.87) are addressed so that the government isn't locked out from using the model in the S-DR across the lifecycle. For commercial models, we negotiate for needed licenses, access to interfaces, or escrow of source code if possible. At minimum, the wrapper will include a mechanism for validation, e.g., test cases or reference outputs provided by the model supplier, to allow ongoing VV&A without needing full source code. We also document the provenance of adopted models (origin, version, modifications made in wrapping) in the model's metadata. This practice aligns with digital engineering best practices to obtain appropriate data rights and documentation during contracting, ensuring that any externally sourced model can be maintained or replaced on our terms.

A5.9. Upgrade and Replacement Strategy. The adopt-and-wrap approach inherently supports future upgrades. If the external model's vendor releases a new version or an alternative solution emerges, we can evaluate it and update the wrapper or swap out the model behind the wrapper, without disrupting the rest of S-DR. The interface presented to our environment remains consistent, so other components are unaffected by the change. This modularity is intentional: it avoids vendor lock-in and allows a continuous inject state-of-the-art technology. However, any new or updated adoption will undergo full VV&A before activation. In cases where an adopted model eventually fails to meet evolving needs (e.g., performance limitations or obsolete technology), the wrapper can be retired along with the model and replaced by an in-house model, again using the same interface. Thus, "adopt-and-wrap" not only expedites initial development by leveraging existing tech, but also provides a controlled path to evolve or phase out those components under governance oversight.