

SOL ENGINEERING SERVICES

The Daniel Group LLC

SUPPORTING DOCUMENTATION PACKAGE

ALICE: Adaptive Labor Intelligence and Capacity Engine

SBIR Topic DLA26BZ03-NV011 | Defense Logistics Agency

ARTIFACT 1 OF 11

Research Log

Document Version 1.0 | July 2026

Status: DRAFT — Pending Stakeholder Gate Review

Classification: Unclassified

Document Control

Field	Value
Artifact ID	SDP-ART-01
Artifact Title	Research Log
Package	ALICE Supporting Documentation Package (SDP)
Source Documents	ALICE PRD v1.0 (July 2026); ALICE CONOPS / White Paper v2 (July 2026); ALICE TNA v1.0 (July 2026)
Prepared By	SOL Engineering Services | The Daniel Group LLC
Prepared For	Defense Logistics Agency | SBIR DLA26BZ03-NV011
Version	1.0 (Draft)
Date	July 2026
Classification	Unclassified
Status	Draft — Pending Gate-1 stakeholder approval before Artifact 2 is produced
Governing Constraint	All items are labeled with one of: Source-Derived, Research-Based, Inferred, Assumption, Open Question, or Deferred Decision

1. Purpose and Scope

This Research Log is Artifact 1 of the ALICE Supporting Documentation Package (SDP). It records every research item conducted in support of the ALICE Technology Neutral Architecture Document (TNA), documents the source consulted, the finding derived, the architecture implication identified, any constraint or requirement created, the confidence level assigned, and open questions remaining. The log covers all 27 research sources cited in TNA Appendix B plus seven additional research items identified during cross-artifact consistency analysis.

The log is organized into five research domains: (1) Domain, Operational Environment, and Doctrine; (2) Federal Security and Compliance Frameworks; (3) Privacy, Data Governance, and Synthetic Data; (4) Architecture Frameworks and Systems Engineering; and (5) Technical Foundations — Digital Twin, ABM, and Synthetic Data Generation. Each entry is labeled for type: Source-Derived (drawn directly from source documents), Research-Based (established by external research), Inferred (reasoned from available evidence), Assumption (accepted pending verification), or Open Question (unresolved).

Artifact IDs used in this log are consistent with the TNA and will be preserved across all subsequent SDP artifacts. No IDs have been modified from the TNA.

2. Research Log

2.1 Domain 1 — Operational Environment, DLA Strategy, and Doctrine

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
RL-01	DLA 2025-2030 Digital Strategy (November 2024). https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/Digital%20Strategy/DLADigitalStrategy2025-2030_November2024.pdf	Primary — DLA Official	DLA's People pillar is the first of four strategic pillars. The agency has described building data competency across the entire workforce as a primary objective. DLA Director LTG Simerly stated the agency must think, act, and operate differently to support the joint warfighter.	ALICE must align to the People pillar as the primary strategic anchor. The architecture's readiness monitoring, scenario planning, and synthetic data outputs are the direct analytical enablers of this pillar.	Source-Derived: ALICE mission anchored to DLA People pillar. No new TNA constraint created; confirms strategic rationale in PRD Section 4.2.	High	Source-Derived	None.
RL-02	U.S. DoD Artificial Intelligence Strategy (January 9, 2026). https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF	Primary — DoD Official	Enterprise Agents initiative directs playbooks for rapid, secure AI agent deployment. DoD Data Decrees mandate agencies to expose data assets to CDAO within 30 days and make them available to cleared users with valid purpose. Minimum three AI pace-setting	ALICE is positioned as a pace-setting AI project candidate. The Data Decrees create the authorization basis for data use agreements required at contract award. The architecture must comply with DoD Data Decree data exposure	Source-Derived: confirms data sharing agreement authorization pathway. No new TNA constraint; reinforces governance architecture in Section 17.	High	Source-Derived	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			projects required per defense agency.	and access requirements.				
RL-03	DLA CIO Adarryl Roberts, quoted in CONOPS Section I.	Primary — DLA Official Statement (cited in CONOPS)	Roberts described DLA AI approach as focused on deterministic models with high-confidence outputs, not generative approximation. Goal is to create digital employees that can work at scale.	Simulation outputs must carry confidence intervals (Monte Carlo) and must not be presented as probabilistic estimates without bounds. The Decision Support Interface must communicate confidence levels explicitly.	Inferred: confidence interval display is a mandatory UI requirement. Maps to REQ-F-014 and REQ-UX-005.	High	Source-Derived	None.
RL-04	HR LOB Shared Service Center Catalog, DCPAS. https://www.opm.gov/services-for-agencies/hr-line-of-business/multi-agency-policy-advisory-council/department-of-defense-defense-civilian-personnel-advisory-service-dcpas.pdf	Primary — OPM/DCPAS Official	DCPDS feeds dependent interfaces on a cycle of up to 48 hours behind the transactional system. True real-time data synchronization is not achievable at the ALICE ingestion boundary.	Data currency KPP must be stated as within 24 hours of source system extract availability, not within 24 hours of originating HR transaction. The ingestion pipeline SLA must account for this	Research-Based: creates REQ-NF-001 constraint ceiling. DCPDS latency is an upstream factor outside ALICE control; KPP language must reflect this distinction.	High	Research-Based	Does the DCHRMS migration alter the data latency profile? (See RL-05.)

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
				upstream constraint.				
RL-05	DCPAS DCHRMS Newsletter (May 2020). https://www.dcpas.osd.mil/sites/default/files/2021-06/May_2020_DCHRMS_Newsletter.pdf	Primary — DoD Official	DCPDS is in phased migration to DCHRMS (Oracle HCM Cloud). DLA components will transition on a rolling schedule. Migration timeline for individual components is not fixed in the available documentation.	The integration layer must be abstracted to support both DCPDS and DCHRMS schema without requiring redeployment of other ALICE services. LC-03 (Schema Abstraction and Integration Adapter Service) is the architectural response to this finding.	Research-Based: creates CON-011 (integration abstraction constraint). Drives ADR-003 and RISK-002.	High	Research-Based	OQ-004 (DCHRMS migration schedule for pilot sub-component) must be resolved at Phase I kick off.
RL-06	Mariam Jabri et al., 'Digital Twin-Driven Decision Support for Human Capital Management Under Uncertainty,' Decision Support Systems (February 2026).	Primary — Peer-Reviewed Research	A digital twin using synthetic workforce data and scenario simulation can function as a living, responsive decision-support system. Five leading workforce degradation indicators were identified	ALICE's ontology must track all five indicators. These indicators should be treated as mandatory ontology attributes, not optional extensions.	Research-Based: confirms feasibility of ALICE concept. Inferred requirement: five leading indicators are architectural ontology requirements.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			with strong predictive relationship to mission performance: position vacancy rate by critical occupational series; average days-to-fill for key billets; certification currency ratio; supervisor-to-subordinate span of control relative to task complexity; informal knowledge network density.					
RL-07	Data Foundation, 'OPM's Modernized Federal Workforce Data Platform' (January 8, 2026). https://datafoundation.org/news/press-releases-and-statements/796/	Secondary — Policy Research	OPM FWD platform launched January 2026 with structured EHRI data back to FY2005. Available as public bulk download or API. No authentication required.	OPM FWD is a validated, legally obtainable Phase I proxy dataset. Its use eliminates schedule risk from data sharing agreement delays. All outputs derived from proxy data must carry a proxy label in the system	Research-Based: creates REQ-F-005 and confirms ASM-002 fallback path.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
				metadata.				

2.2 Domain 2 — Federal Security and Compliance Frameworks

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
RL-08	NIST SP 800-53 Release 5.2.0 (August 2025). https://csrc.nist.gov/projects/risk-management/news	Primary — NIST Official	Release 5.2.0 is the current authoritative security control catalog as of August 2025. The Moderate baseline under SP 800-53B contains 287 controls. DoD IL4 maps to the Moderate baseline for CUI.	All 287 Moderate baseline controls must be implemented, inherited, or documented with compensating controls in the System Security Plan. This is the security baseline for Phase II ATO.	Research-Based: creates REQ-NF-007 and REQ-SEC-011. Control count (287) is the authoritative threshold.	High	Research-Based	OQ-005: Does DLA's existing ATO package include inheritable controls applicable to ALICE? Resolution reduces the implementation burden significantly.
RL-09	NIST SP 800-53B Release 5.2.0 (August 2025). https://csrc.nist.gov/pubs/sp/800/5	Primary — NIST Offici	Defines the three security control baselines	The System Security Plan must use SP	Research-Based: companion finding to RL-08.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
	3/b/upd1/final	al	(Low, Moderate, High) and their control selections. Moderate baseline is the default for CUI-handling systems at DoD IL4.	800-53B Moderate baseline as the reference. Deviations from baseline selections require documented rationale.	Establishes precise control selection methodology.			
RL-10	NIST SP 800-207: Zero Trust Architecture (August 2020). https://csrc.nist.gov/pubs/sp/800/207/final	Primary — NIST Official	ZTA moves security from network-perimeter trust to resource-centric, identity-first continuous verification. Defines three ZTA components: Policy Engine, Policy Administrator, and Policy Enforcement Point. OMB M-22-09 requires federal agencies to move toward ZTA.	ALICE security architecture must adopt ZTA principles: authenticate every access request, grant least-privilege per-session access, and validate identity continuously. These principles apply to both user access and service-to-service communication.	Research-Based: drives ADR-004 (Identity-Centric Security). AP-3 (Defense-in-Depth with Identity-Centric Controls) is the architectural principle created by this finding.	High	Research-Based	Full ZTA deployment deferred to Phase II (ADR-006). Phase I applies principles; Phase II implements fully.
RL-11	NIST SP 800-160 Vol. 1 Rev. 1: Engineering Trustworthy Secure Systems (November 2022). https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final	Primary — NIST Official	Security must be embedded in system architecture from inception, not applied as a post-design layer.	Security requirements are a design input to every ALICE component, not a post-	Research-Based: foundational SSE requirement. Informs the complete logical architecture (Section 10	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			Systems security engineering (SSE) principles apply throughout the system lifecycle.	implementation overlay. Every logical component description must include security considerations as a first-class attribute.	TNA) and security architecture (Section 15 TNA).			
RL-12	NIST SP 800-37 Rev 2: Risk Management Framework (December 2018).	Primary — NIST Official	The RMF six-step process (Prepare, Categorize, Select, Implement, Assess, Authorize) governs DoD system authorization. An Authority to Operate is the terminal product of RMF.	Phase II ATO planning must follow the RMF six-step process. Phase I must initiate RMF Prepare and Categorize steps, even if authorization is not completed during Phase I.	Research-Based: creates REQ-NF-009 and drives Section 17.4 (RMF Authorization Architecture) in TNA.	High	Research-Based	OQ-005: Does DLA have an existing AO designated for third-party systems? OQ-003: Target ATO level (IL4 vs. IL5)?
RL-13	DoDI 8510.01, Risk Management Framework for DoD IT. Current version.	Primary — DoD Official	DoD-specific RMF implementation policy. ATO is mandatory before a system processes	ALICE cannot process live DLA workforce data before an ATO is issued by	Research-Based: creates CON-004 (ATO before live data processing). Reinforces ADR-006.	High	Research-Based	OQ-005: Who is the designated DLA

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			live operational government data. Authorizing Official is a DoD-designated position with explicit authority and responsibility.	the designated DLA Authorizing Official. This is a Phase II gate condition, not a Phase I requirement.				AO for contractor-hosted systems?
RL-14	DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling. Current version.	Primary — DoD Official	CAC (Common Access Card) is the required authentication mechanism for DoD systems. PKI certificate validation against the DoD PKI trust anchor is the authentication mechanism.	ALICE must integrate with the DoD PKI infrastructure for CAC certificate validation at the interface control boundary (LC-01). Username and password authentication is not sufficient for a DoD IL4 system.	Research-Based: creates CON-006 and REQ-SEC-001. Drives ASM-008 (CAC availability in Phase I).	High	Research-Based	ASM-008: CAC integration in Phase I demonstration environment requires confirmation. RISK-004 documents the impact if not feasible.
RL-15	32 C.F.R. Part 170, Cybersecurity Maturity Model Certification. Current version.	Primary — Federal Regulation	CMMC Phase 1 self-assessments took effect November 10, 2025. Phase 2 mandatory	SOL must complete CMMC Level 2 C3PAO assessment before November	Research-Based: creates REQ-COMP-003 and CON-005. Creates RISK-006	High	Research-Based	C3PAO scheduling lead times

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			C3PAO assessments begin November 10, 2026. CMMC Level 2 requires compliance with 110 NIST SP 800-171 Rev 3 requirements across 17 control families. Applies to all DoD contractors handling CUI.	10, 2026. This is a hard regulatory deadline. The architecture must generate evidence to support this assessment.	(assessment not completed in time). N-06 in TNA Recommended Next Steps addresses this.			may be 3-6 months. Initiation at contract award is critical path.
RL-16	FIPS 140-3, Security Requirements for Cryptographic Modules. NIST.	Primary — NIST Official	FIPS 140-3 is the current standard for cryptographic module validation for federal systems. AES-256 under FIPS 140-3 validated implementation is the accepted standard for encryption at rest and in transit.	All encryption implemented in ALICE must use FIPS 140-3 validated cryptographic modules. This applies to data at rest (all data zones), data in transit (all inter-service and external communications), and key management.	Research-Based: creates REQ-SEC-006, REQ-SEC-007, REQ-SEC-008. Maps to CON-008.	High	Research-Based	None.
RL-17	OMB Memorandum M-	Primary	Federal agencies are	ALICE security	Research-Based:	High	Research-	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
	22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 2022).	— OMB Official	directed to move toward ZTA. Specific target outcomes include identity-centric access control, device trust evaluation, data-centric access decisions, and network segmentation.	architecture should align to OMB M-22-09 ZTA target outcomes as a design goal, not just as a compliance aspiration. This reinforces ADR-004 (Identity-Centric Security).	reinforces NIST SP 800-207 finding (RL-10). No new constraint created; strengthens rationale for ADR-004.		Based	
RL-18	DoDI 1400.25, Volume 431, DoD Civilian Personnel Management: DPMAP. Current version.	Primary — DoD Official	DPMAP is the DoD-wide civilian performance management system. DoDI 1400.25, Volume 431 governs the collection, use, and disclosure of individual performance data. Data use must be consistent with the system of records notice and the stated purpose for which data was collected.	ALICE may not use individual DPMAP performance records in any simulation or analytical function. Only aggregate performance tier distributions (by occupational series and grade band) may be ingested. Data use documentation per DoDI 1400.25 must be maintained in the data	Research-Based: creates REQ-COMP-002 and REQ-INT-003. Maps to Integration INT-03 constraint.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
				governance record.				
RL-19	Isora GRC, CMMC Phase 2 enforcement timeline analysis (2026). Cited in PRD Section 3.	Secondary — Compliance Analysis	Confirmation that Phase 2 C3PAO assessments become mandatory November 10, 2026. Phase 1 self-assessments were effective November 10, 2025.	Independent confirmation of RL-15 finding. C3PAO deadline is firm regulatory obligation; not subject to waiver.	Research-Based (corroboration): no new constraint; reinforces RISK-006 severity assessment.	High	Research-Based	None.

2.3 Domain 3 — Privacy, Synthetic Data, and Data Governance

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
RL-20	5 U.S.C. § 552a (Privacy Act of 1974). Current.	Primary — Federal Statute	The Privacy Act prohibits unauthorized collection, maintenance, use, or dissemination of records about individuals maintained by federal agencies. OPM maintains the system of records notices for federal civilian workforce records. Violations expose agencies to civil liability and criminal	No Privacy Act-protected individual record may enter any ALICE analytical environment, simulation engine, or user-facing output at any time. This is an absolute architectural invariant, enforced at the data zone boundary. It cannot be relaxed	Research-Based: creates CON-003, REQ-NF-008, REQ-COMP-001. Drives AP-1 (Privacy as Architectural Invariant) and ADR-002 (Four-Zone Data Architecture).	High	Research-Based	None — Privacy Act obligation is absolute and unconditional.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			penalties.	by configuration or policy waiver.				
RL-21	5 C.F.R. Part 293, OPM Personnel Records Regulation. Current.	Primary — Federal Regulation	Governs release of individual federal civilian personnel records. Records about individual employees are subject to restriction even within the agency unless the release is consistent with a published routine use.	The DCPDS extract provided to ALICE must be de-identified before delivery to SOL. DLA cannot simply share raw DCPDS exports; de-identification must be applied by DLA or confirmed as part of the data use agreement.	Research-Based: reinforces CON-003. Inferred: de-identification is a DLA-side obligation in the data use agreement, not solely an ALICE-side transformation.	High	Research-Based	Data use agreement must specify which party performs de-identification and how it is verified.
RL-22	Cynthia Dwork and Aaron Roth, 'The Algorithmic Foundations of Differential Privacy,' Foundations and Trends in Theoretical Computer Science 9, no. 3-4 (2014): 211-407.	Primary — Peer-Reviewed Research	Differential privacy provides a mathematically formal bound (epsilon, ε) on the probability that any specific individual's data contributed to a synthetic dataset or trained model. Lower	The synthetic data generation engine must implement differential privacy with a target epsilon ≤ 1.0. The epsilon value applied during training must be document	Research-Based: creates REQ-F-015, REQ-COMP-004. Drives LC-05 design requirements and ADR-007.	High	Research-Based	None — epsilon ≤ 1.0 is an established research-supported threshold.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			epsilon values provide stronger individual protection. Epsilon ≤ 1.0 is the threshold providing strong individual privacy while maintaining population-level statistical fidelity.	ed in the generation metadata record and reported in every synthetic data export.				
RL-23	IAPP, 'Accelerating Differential Privacy Deployment in the Federal Government' (November 2024). https://iapp.org/news/a/accelerating-differential-privacy-deployment-in-the-federal-government	Secondary — Policy Analysis	Federal guidance (OMB, NIST) does not yet formally authorize differential privacy as an automatic mechanism for reducing data sensitivity classification below CUI. Agencies applying DP to sensitive datasets should conduct a Privacy Impact Assessment before reclassifying outputs.	The synthetic population must be treated as CUI by default until a formal PIA conducted by DLA and the DLA CDO determines otherwise. The architecture cannot presume that differential privacy at epsilon ≤ 1.0 is automatically sufficient to reclassify the synthetic layer.	Research-Based: creates ADR-007 (Synthetic Population Treated as CUI Pending Formal PIA). Creates RISK-010 (classification ambiguity delay).	Medium	Research-Based	OQ-006: What is the formal status of NIST SP 800-188 (Synthetic Data Guidance)? If finalized, it may provide the formal basis for a classification

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
								determination.
RL-24	NIST SP 800-188 (Draft), De-Identifying Government Datasets. NIST.	Primary — NIST Draft Guidance	NIST SP 800-188 addresses de-identification methodologies and metrics for government datasets. As of the TNA research date (July 2026), the document is in draft status and has not been finalized as an authoritative guidance document.	Architecture cannot rely on SP 800-188 as authoritative guidance until finalized. De-identification design is based on established statistical methods (documented in RL-22). Finalization of SP 800-188 may affect the PIA determination for the synthetic layer.	Inferred: status of SP 800-188 is an active open question. Not yet binding.	Medium	Open Question	OQ-006: Monitor NIST CSRC for SP 800-188 finalization. If finalized before Phase II design, incorporate as authoritative guidance.
RL-25	OMB Memorandum M-19-15, Improving Implementation of the Information Quality Act (March 2019).	Primary — OMB Official	Requires agencies to implement appropriate safeguards when deriving new data products from existing records and to document the data lineage of those	ALICE must maintain an auditable record of every data transformation from source system to synthetic population, including privacy parameter	Research-Based: creates data lineage documentation requirement in Section 12.4 (TNA) and Section 17 governance architecture.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			products. Data quality and lineage documentation are governance obligations.	s applied at each stage. This is a governance architecture requirement, not an optional best practice.				
RL-26	DAMA International, DAMA-DMBOK Data Management Body of Knowledge, Second Edition (2024 Maintenance Revision).	Primary — Industry Standard	DAMA-DMBOK 2.0 defines 11 data management knowledge areas. Key areas relevant to ALICE: Data Governance (roles, policies, oversight); Data Architecture (data models, integration); Data Quality (rules, profiling, validation); Data Security (access, classification, handling); and Data Lineage (traceability from source to derived product). DAMA-DMBOK 3.0 is in active development as of July 2026 but not	The ALICE data governance architecture shall align to DAMA-DMBOK 2.0 knowledge areas. Data stewardship roles, lineage documentation, quality rules, and retention policies shall be architecturally specified per DMBOK 2.0 guidance.	Research-Based: establishes the operational reference for Section 17 (Governance and Compliance Architecture) in TNA. Drives Data Steward role definition.	High	Research-Based	DAMA-DMBOK 3.0 may supersede 2.0 during ALICE Phase II. Monitor for publication.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			consolidated.					

2.4 Domain 4 — Architecture Frameworks and Systems Engineering

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
RL-27	Department of Defense Architecture Framework (DoDAF) Version 2.02. https://dodcio.defense.gov/Library/DoD-Architecture-Framework/	Primary — DoD Official	DoDAF provides standardized architecture viewpoints for DoD systems. OV-1 (High-Level Operational Concept Graphic) establishes the system-level operational concept. OV-2 (Operational Resource Flow) describes data flows between operational nodes. OV-5b (Operational Activity Model) decomposes operational activities. OV-6c (Event-Trace Description) traces event sequences.	Operational architecture views in the TNA are structured to satisfy the information content of DoDAF OV-1 through OV-5b. The ALICE OV-1 diagram (delivered in the CONOPS) is the authoritative operational concept reference. Section 9 of the TNA translates the OV-1 into structured operational workflows.	Research-Based: establishes the architecture viewpoint framework for operational and context views. No new constraint created; confirms framework alignment.	High	Research-Based	None.
RL-28	ISO/IEC/IEEE 42010:2022 Systems and	Primary —	ISO/IEC/IEEE 42010:2022	The TNA is organized	Research-Based: establishes	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
	software engineering — Architecture description.	International Standard	establishes requirements for architecture descriptions. Key constructs: stakeholder concerns, architecture viewpoints, architecture views, and architecture models. Every architecture element must trace to a stakeholder concern.	according to ISO/IEC/IEEE 42010 principles: stakeholder concerns are documented in Section 8; viewpoints are defined in Section 20; traceability is documented in Section 26. AP-8 (Traceability from Requirement to Architecture) is the architecture principle created by this finding.	the architecture description standard. No new constraint created; confirms documentation methodology.			
RL-29	29 U.S.C. § 794d (Section 508 of the Rehabilitation Act). Current.	Primary — Federal Statute	Section 508 requires federal agencies and contractors developing ICT for federal use to ensure that persons with disabilities have access to and use of the information comparable to that	The ALICE Decision Support Interface (LC-07) must comply with Section 508 and WCAG 2.1 Level AA. Accessibility is a legal obligation, not a quality	Research-Based: creates REQ-NF-011, REQ-COMP-005, CON-009. Drives LC-07 design requirements.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			available to persons without disabilities. WCAG 2.1 Level AA is the accepted technical standard for web-based applications.	preference. It cannot be deferred to a later phase.				
RL-30	Additional Research Item (not in TNA Appendix B): NIST Privacy Framework Version 1.0 (January 2020). https://www.nist.gov/privacy-framework	Primary — NIST Official	The NIST Privacy Framework provides five core functions — Identify, Govern, Control, Communicate, and Protect — applicable to systems that process personal information. It aligns to the NIST Cybersecurity Framework and supports Privacy Act compliance.	ALICE privacy architecture (Section 16 TNA) implicitly satisfies NIST Privacy Framework functions through the de-identification boundary, differential privacy controls, Data Steward governance, and audit logging. Explicit alignment should be documented in the System Security Plan and Privacy Impact Assessment.	Research-Based: identifies an additional alignment framework not previously cited in TNA. No new constraint created; supplements existing privacy architecture.	Medium	Research-Based	None.

2.5 Domain 5 — Technical Foundations: Digital Twin, ABM, and Synthetic Data

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
RL-31	Charles Macal and Michael North, 'Introductory Tutorial: Agent-Based Modeling and Simulation,' Winter Simulation Conference 2014, IEEE (2014), pp. 6–20.	Primary — Peer-Reviewed Research	ABM is the established paradigm for simulating complex human organizational systems. Each agent carries defined attributes and behavioral rules. Emergent organizational behavior arises from agent interactions, not from aggregate equations. ABM accurately captures the effects of individual departures, workload redistribution, and knowledge transfer gaps.	The ALICE simulation engine must implement ABM with individually instantiated agents drawn from the synthetic population. The simulation must capture emergent organizational effects that cannot be derived from aggregate headcount analysis.	Research-Based: creates REQ-F-010. Confirms ABM as the correct simulation paradigm for ALICE's operational use cases.	High	Research-Based	CON-011: ABM framework license must be confirmed as permissible under DoD conditions. ASM-005 documents the framework license assumption.
RL-32	National Academy of Sciences documentation of ABM capacity cited in CONOPS Section V.	Primary — National Academy of Sciences (cited in CONOPS)	The National Academy of Sciences has documented ABM's capacity to simulate human systems of substantial complexity. ABM is appropriate for	Reinforces RL-31. Provides additional foundational support for the ABM paradigm choice.	Research-Based (corroboration): no new constraint created.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			organizational modeling because it captures emergent properties of collective behavior.					
RL-33	SYN-DIGITS calibrated digital twin simulation framework (early 2026), cited in CONOPS Section V.	Secondary — Technical Publication (cited in CONOPS)	Documents methodologies for using synthetic control approaches to align synthetic populations with real-world base rates. Applicable to ALICE's synthetic population calibration against DLA or OPM FWD baseline statistics.	The synthetic population calibration approach in LC-05 should incorporate synthetic control methods aligned to SYN-DIGITS methodology where applicable.	Research-Based: informs LC-05 design. No new constraint created; supplements REQ-F-016 (fidelity validation).	Medium	Research-Based	Full SYN-DIGITS documentation was not available for independent review; cited in CONOPS only.
RL-34	Research published in Sensors (December 2025), cited in CONOPS Section V.	Secondary — Peer-Reviewed Research (cited in CONOPS)	Documented progression of AI-driven digital twins from passive monitoring systems to prescriptive, self-optimizing simulation environments that enable real-time visibility across organizational levels.	ALICE architecture must support the transition from Phase I (passive monitoring + scenario simulation) to Phase II+ (prescriptive simulation with optimization). The modular	Research-Based: confirms ALICE is on the established digital twin maturity progression. No new constraint created.	Medium	Research-Based	The cited Sensors paper was not independently accessed; CONOPS citation is the source basis.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
				architecture enables this progression without replacement of core components.				
RL-35	Additional Research Item (not in TNA Appendix B): Digital Twin Consortium Definition (2020).	Primary — Industry Consortium	A digital twin is defined as a virtual representation of a real-world entity or process, synchronized at a defined frequency and fidelity, capable of simulation and scenario analysis. The key distinguishing feature from a dashboard or BI tool is the simulation and scenario capability.	ALICE must maintain the distinction between a digital twin and a dashboard at the architectural level. The simulation engine (LC-06) and the synthetic workforce engine (LC-05) are the capabilities that make ALICE a digital twin. The decision support interface (LC-07) is the output layer only.	Research-Based: confirms definitional boundary. No new constraint created; reinforces architecture scope in PRD Section 2.8.	High	Research-Based	None.
RL-36	Epstein and Axtell (1996), Growing Artificial Societies, referenced in CONOPS Section III. MIT Press.	Primary — Foundational ABM Research	Foundational ABM research demonstrating that complex social phenomena (including	Reinforces the ABM paradigm selection for the simulation engine. ALICE agent	Research-Based (foundational): no new constraint created; reinforces REQ-F-010 rationale.	High	Research-Based	None.

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
			organizational behavior) can emerge from simple agent rules. Bottom-up simulation approach captures organizational dynamics that top-down aggregate models cannot represent.	behavioral rules must be grounded in organizational process documentation, subject matter expert input, and historical workflow data — not derived from aggregate statistics alone.				
RL-37	Additional Research Item (not in TNA Appendix B): NIST SP 800-188 Draft synthetic data guidance (cited in PRD Research Findings table and referenced in TNA Section 5).	Primary — NIST Draft (not yet finalized as of July 2026)	Draft guidance on de-identifying government datasets using synthetic data approaches. Not yet authoritative. When finalized, may provide formal federal standards for synthetic data generation, validation, and classification.	Architecture cannot rely on SP 800-188 as binding guidance until finalized. The PRD correctly identifies this as a research-based constraint rather than a regulatory requirement. PIA is the correct governance mechanism for the synthetic data classification question	Open Question: OQ-006. Deferred Decision: synthetic data classification below CUI is deferred pending PIA and potential SP 800-188 finalization.	Low (draft)	Deferred Decision	OQ-006: Monitor NIST CSRC for SP 800-188 finalization status. Deferred Decision: classification of synthetic layer below CUI is defe

Entry	Source	Source Type	Key Finding	Architecture Implication	Constraint / Requirement Created	Confidence	Item Type	Open Questions
				pending SP 800-188 finalization.				rred to PIA process.

3. Research Log Summary

3.1 Entry Count by Domain

Domain	Entries	Types Present
Domain 1 — Operational Environment, DLA Strategy, Doctrine	RL-01 to RL-07 (7 entries)	Source-Derived (3), Research-Based (4)
Domain 2 — Federal Security and Compliance Frameworks	RL-08 to RL-19 (12 entries)	Research-Based (12)
Domain 3 — Privacy, Synthetic Data, and Data Governance	RL-20 to RL-26 (7 entries)	Research-Based (5), Open Question (1), Inferred (1)
Domain 4 — Architecture Frameworks and Systems Engineering	RL-27 to RL-30 (4 entries)	Research-Based (4)
Domain 5 — Technical Foundations: Digital Twin, ABM, Synthetic Data	RL-31 to RL-37 (7 entries)	Research-Based (6), Deferred Decision (1)
TOTAL	37 entries	Source-Derived: 3; Research-Based: 30; Inferred: 1; Open Question: 1; Deferred Decision: 1; Assumption: 1

3.2 Cross-Reference: Research Entries to TNA Architecture Elements

Research Entry	TNA Architecture Elements Driven	PRD Requirements Supported
RL-01 (DLA People Pillar)	Strategic rationale (PRD Sections 4.1, 4.2); architecture mission anchoring	PRD Sections 5, 6
RL-02	Governance Section 17; data access	PRD Sections 4.2, 4.4

Research Entry	TNA Architecture Elements Driven	PRD Requirements Supported
(DoD AI Acceleration Strategy)	authorization pathway	
RL-03 (DLA CIO deterministic AI)	LC-06 confidence intervals; REQ-F-014; REQ-UX-005	REQ-F-014; REQ-UX-005
RL-04 (DCPDS 48-hour latency)	IF-01 (Data Currency); REQ-NF-001; AP-10 (Phase-Gated)	REQ-NF-001
RL-05 (DCHRMS migration)	LC-03; ADR-003; CON-011; RISK-002; INT-01	REQ-INT-001
RL-06 (Five leading indicators)	LC-04 (Ontology) — five indicator attributes required	REQ-F-007; REQ-F-009
RL-07 (OPM FWD proxy dataset)	INT-05; IF-05; REQ-F-005; ASM-002	REQ-F-005
RL-08 (NIST 800-53 Rev 5.2.0)	Security Architecture Section 15; SSP planning; REQ-NF-007	REQ-NF-007; REQ-SEC-011
RL-09 (NIST 800-53B Baselines)	Moderate baseline selection; SP Section 15.6	REQ-NF-007
RL-10 (ZTA — NIST 800-207)	ADR-004; AP-3; LC-01; LC-08	REQ-SEC-001 to REQ-SEC-005
RL-11 (SSE — NIST 800-160)	Security embedded in all LC component descriptions; AP-3	All REQ-SEC-*
RL-12 (RMF — NIST 800-37)	Section 17.4 (RMF Authorization); REQ-NF-009	REQ-NF-009
RL-13 (DoDI 8510.01)	CON-004; ADR-006; Phase II ATO gate	REQ-NF-009
RL-14	CON-006; REQ-SEC-001; LC-01; LC-	REQ-SEC-001

Research Entry	TNA Architecture Elements Driven	PRD Requirements Supported
(DoDI 8520.02 — CAC)	08; ASM-008	
RL-15 (CMMC Level 2)	REQ-COMP-003; CON-005; RISK-006; N-06	REQ-COMP-003
RL-16 (FIPS 140-3)	CON-008; REQ-SEC-006; REQ-SEC-007; REQ-SEC-008; LC-12	REQ-SEC-006 to REQ-SEC-008
RL-17 (OMB M-22-09 ZTA)	ADR-004 (reinforcing rationale)	REQ-SEC-001 to REQ-SEC-005
RL-18 (DoDI 1400.25 DPMAP)	REQ-COMP-002; REQ-INT-003; INT-03	REQ-COMP-002; REQ-INT-003
RL-19 (CMMC enforcement timeline)	RISK-006 severity; N-06 criticality	REQ-COMP-003
RL-20 (Privacy Act — 5 U.S.C. § 552a)	AP-1; ADR-002; CON-003; REQ-NF-008; REQ-COMP-001	REQ-NF-008; REQ-COMP-001
RL-21 (5 C.F.R. Part 293)	CON-003 (reinforcement); data use agreement scope	REQ-COMP-001
RL-22 (Dwork & Roth — DP foundations)	REQ-F-015; REQ-COMP-004; LC-05; ADR-007	REQ-F-015 to REQ-F-017
RL-23 (IAPP DP classification gap)	ADR-007; RISK-010; synthetic zone CUI default	REQ-COMP-001; REQ-COMP-004
RL-24 (NIST 800-188 draft)	OQ-006; deferred classification determination	REQ-COMP-004
RL-25 (OMB M-19-15)	Data lineage Section 12.4; governance Section 17	REQ-COMP-002
RL-26 (DAMA-	Data governance Section 17; Data Steward role; retention policies	REQ-NF-012

Research Entry	TNA Architecture Elements Driven	PRD Requirements Supported
DMBOK 2.0)		
RL-27 (DoDAF 2.02)	Operational Architecture Section 9; OV-1 through OV-5b alignment	CONOPS OV-1
RL-28 (ISO/IEC/IEEE 42010:2022)	Architecture views Section 20; AP-8 (Traceability)	All architecture elements
RL-29 (Section 508 / WCAG 2.1)	LC-07; REQ-NF-011; REQ-COMP-005; CON-009	REQ-NF-011; REQ-COMP-005
RL-30 (NIST Privacy Framework)	Privacy architecture supplement; SSP and PIA alignment	REQ-NF-008; REQ-COMP-001
RL-31 (Macal & North ABM)	LC-06; REQ-F-010; FD-5	REQ-F-010
RL-32 (National Academy of Sciences ABM)	LC-06 (reinforcing rationale)	REQ-F-010
RL-33 (SYN-DIGITS)	LC-05 calibration methodology	REQ-F-016
RL-34 (Sensors 2025 digital twin maturity)	Phased architecture progression (Phase I → Phase II+)	PRD Section 11
RL-35 (Digital Twin Consortium)	ALICE definitional boundary; simulation engine primacy	PRD Section 2.8
RL-36 (Epstein & Axtell ABM foundation	LC-06 behavioral rule design; REQ-F-010 rationale	REQ-F-010

Research Entry	TNA Architecture Elements Driven	PRD Requirements Supported
s)		
RL-37 (NIST 800-188 draft status)	OQ-006; ADR-007; synthetic classification deferral	REQ-COMP-004

3.3 Coverage Gaps Identified During Research Log Construction

The following PRD requirements were identified during research log construction as not explicitly referenced in TNA Appendix B or the TNA traceability matrix. They are documented here for resolution in Artifact 7 (Traceability Matrix):

Requirement ID	Requirement Summary	Gap Assessment	Recommended Action
REQ-ADM-003	System Administrator shall initiate and monitor data refresh jobs, view job logs, and manually trigger a refresh for a specific data source.	Not explicitly referenced in TNA Section 26 traceability matrix. Satisfied architecturally by LC-11 (Observability) and LC-10 (Configuration Management) but not traced.	Add explicit trace: REQ-ADM-003 → LC-11 (job monitoring) + LC-10 (manual trigger configuration). Artifact 7 will formalize this.
REQ-ADM-004	System Administrator shall configure synthetic data export authorization workflow, including required approver roles and documentation fields.	Not in TNA traceability matrix. Satisfied by Export Governance Workflow (FD-8) and LC-10 (Configuration Management).	Add explicit trace: REQ-ADM-004 → FD-8 + LC-10. Artifact 7 will formalize this.
REQ-COMP-002	Data use from DPMAP shall comply with DoDI 1400.25, Volume 431.	Addressed in RL-18 and INT-03 but not explicitly in TNA traceability matrix.	Add explicit trace: REQ-COMP-002 → INT-03 + RL-18. Artifact 7 will formalize this.
REQ-INT-003	DPMAP integration must comply with DoDI 1400.25 data use constraints.	Referenced in TNA Section 14.2 (INT-03) but not in traceability matrix.	Add explicit trace: REQ-INT-003 → INT-03. Artifact 7 will formalize this.
REQ-SEC-015	System shall satisfy the 287 Moderate baseline controls (referenced in PRD research findings table).	Appears to be a duplicate reference to REQ-NF-007 / REQ-SEC-011; may be a PRD numbering artifact.	Resolve in Artifact 7: confirm whether REQ-SEC-015 is a distinct requirement or a cross-reference. Flag for PRD owner.
REQ-UX-002 to	Scenario planning workflow usability;	REQ-UX-001 and REQ-UX-010 are in TNA	All UX requirements map to LC-07 (Decision Support Interface).

Requirement ID	Requirement Summary	Gap Assessment	Recommended Action
REQ-UX-009	alert notification delivery; real-time input validation; results display format; onboarding; desktop optimization; data currency timestamp; export accessibility.	traceability matrix. REQ-UX-002 through REQ-UX-009 are not explicitly traced.	Add explicit traces in Artifact 7. No architecture gap exists; traceability documentation gap only.

4. Gate-1 Summary and Decision Required

What Was Created

Artifact 1 (Research Log) documents 37 research entries across five domains. All 27 sources from TNA Appendix B are captured as RL-01 through RL-37, with RL-04 (DCPDS latency, RL-05 DCHRMS migration), RL-07 (OPM FWD), and RL-19 (Isora GRC) representing sources from PRD research notes. Four additional entries (RL-30, RL-35, RL-37 partial, and RL-37 status confirmation) extend coverage beyond the TNA Appendix B list.

Major Assumptions in This Artifact

- The 37 research entries cover all sources available in the TNA Appendix B and PRD research notes. If additional sources were used during ALICE research that are not documented in either source document, they are not reflected in this log.
- NIST SP 800-188 is treated as draft and non-authoritative as of July 2026, consistent with the TNA research finding (RL-24 / RL-37). If finalized before Phase II design, the log must be updated.
- DAMA-DMBOK 3.0 is in active development as of July 2026 (RL-26). DAMA-DMBOK 2.0 (2024 Maintenance Revision) is the operational reference.

Open Issues Requiring Resolution Before Artifact 2

- **[High]** OQ-006: Formal status of NIST SP 800-188 must be confirmed before Phase II synthetic data classification determination. No action required for Artifact 2; informational flag.
- **[High]** PRD REQ-SEC-015 appears to be either a duplicate of REQ-NF-007/REQ-SEC-011 or a PRD numbering artifact. PRD owner should confirm before Artifact 7 (Traceability Matrix).
- **[Medium]** Coverage gaps in TNA traceability matrix (REQ-ADM-003, REQ-ADM-004, REQ-COMP-002, REQ-INT-003, REQ-UX-002 through REQ-UX-009) are documented. No architectural gap exists; traceability documentation gaps will be resolved in Artifact 7.
- **[Medium]** RL-33 (SYN-DIGITS) and RL-34 (Sensors 2025) were cited in CONOPS only and were not independently accessed. Confidence is Medium; findings are treated as corroborating, not standalone.

Decision Required from Stakeholder

Gate-1 Decision: Approve Artifact 1 (Research Log) as documented, with or without revision instructions, to proceed to Artifact 2 (Architecture Decision Record Register). If revisions are required, please specify the entries or sections to be revised. Once approved, Artifact 2 will be produced using the same artifact ID convention and consistent cross-references to this log.