

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 5 OF 11

Interface Catalog

Document Version 1.0 | July 2026

Status: DRAFT — Pending Gate-5 Stakeholder Review

Classification: Unclassified

Document Control

Field	Value
Artifact ID	SDP-ART-05
Artifact Title	Interface Catalog
Artifact Dependencies	SDP-ART-01 through SDP-ART-04 — all approved
Package	ALICE Supporting Documentation Package (SDP)
Source Documents	ALICE TNA v1.0 Sections 13, 14; ALICE PRD v1.0 Sections 15, 16, 18, 19; SDP-ART-02; SDP-ART-03; SDP-ART-04
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-5 stakeholder approval before Artifact 6 is produced
Interface Counts	6 external integration interfaces (INT-01 through INT-06); 15 internal information flows (IF-01 through IF-15); 21 interfaces total
ID Convention	All IDs preserved from prior approved artifacts. No IDs modified.

1. Purpose and Scope

This Interface Catalog is Artifact 5 of the ALICE Supporting Documentation Package. It is the authoritative reference for all interfaces in the ALICE system — both external integration interfaces connecting ALICE to source systems and identity infrastructure, and internal information flows connecting service components within the ALICE boundary.

Part A of the catalog covers the six external integration interfaces (INT-01 through INT-06). For each, the catalog documents: the external system, business purpose, data exchanged, interaction direction, Phase I and Phase II interface types, authentication and authorization requirements, data formats, error handling, availability dependency, security classification, audit and logging requirements, associated data entities and components, risk rating, acceptance criteria, and governing ADRs.

Part B of the catalog covers the fifteen internal information flows (IF-01 through IF-15). For each flow, the catalog documents: source and destination components, data exchanged and its classification, trigger and frequency, direction, transport protocol class, validation requirements, transformation requirements, error handling, retry behavior, audit requirements, privacy considerations, associated data entities, and governing ADRs.

Part C provides cross-reference tables mapping interfaces to components, data entities, information flows, and PRD requirements. All interface specifications maintain strict technology neutrality. No specific vendor product, API version, middleware platform, or messaging broker is prescribed. Where protocol classes are named (e.g., encrypted file transfer, synchronous read-only API), they describe capability requirements, not implementation choices.

Items labeled [INFERRED] represent interface requirements reasoned from source documents. Items labeled [OPEN] identify questions requiring stakeholder resolution before the interface can be fully specified for implementation.

2. Interface Architecture Overview

2.1 Interface Taxonomy

Category	Interface IDs	Description	Trust Boundary Crossed?	Phase
External Integrations — Source Systems	INT-01, INT-02, INT-03, INT-04, INT-05	Read-only data pulls from authoritative DLA source systems and OPM public data. ALICE is the consumer; source systems are the providers.	Yes — ALICE boundary to DLA internal network zone or public internet	I and II (INT-01 through INT-04); Phase I only for INT-05
External Integration — Identity	INT-06	DoD PKI / CAC certificate validation for user authentication. Read-only per-session query.	Yes — ALICE boundary to DoD identity infrastructure zone	I and II
Internal Flows — Ingestion Pipeline	IF-01 through IF-09	Data flows from source system receipt through de-identification, zone write, ontology update, and synthetic generation.	No — internal to ALICE boundary	I and II
Internal Flows — Simulation and Decision Support	IF-10, IF-11, IF-12, IF-13	Data flows from the synthetic zone through simulation execution to the decision support interface and alert delivery.	No — internal to ALICE boundary	I and II
Internal Flows — Governance and Audit	IF-14, IF-15	Audit event delivery from all services to LC-09; synthetic data export delivery to authorized requester.	IF-15 crosses ALICE boundary (outbound to authorized recipient)	I and II

2.2 Interface Summary Index

Interface ID	Name	Type	Source	Destination	Trigger	Frequency	Dependency Risk	Data Classification
INT-01	DCPDS / DCHRMS Ingestion	External — Inbound	DCPDS (Phase I) / DCHRMS (Phase II)	LC-03 → LC-02	Scheduled	Daily delta	HIGH	Raw: Privacy Act-protected (in-

Interface ID	Name	Type	Source	Destination	Trigger	Frequency	Dependency Risk	Data Classification
								flight only). Processed: CUI.
INT-02	DLA TMS Ingestion	External — Inbound	DLA Training Management System	LC-03 → LC-02	Scheduled	Weekly	MEDIUM	Raw: Privacy Act-adjacent (in-flight only). Processed: CUI.
INT-03	DPMAP Ingestion	External — Inbound	DPMAP / DCHRMS PM Module	LC-03 → LC-02	Scheduled	Annual	MEDIUM	Aggregate only. No individual records. CUI.
INT-04	EBS Workload Metrics Ingestion	External — Inbound	EBS (SAP DLA)	LC-03 → LC-02	Scheduled	Weekly	MEDIUM	CUI. No PII.
INT-05	OPM FWD Proxy Data Pull	External — Inbound	OPM FWD (data.opm.gov)	LC-02	On-demand	As needed (Phase I proxy)	LOW	Public dataset. Proxy flag set on all derived records.
INT-06	DoD PKI / CAC Authentication	Identity Federation	DoD PKI Authority	LC-01 ↔ LC-08	Per user session	Per session	HIGH	Session credential metadata. No workforce data.
IF-01	Source Data Ingestion (DCPDS/DCHRMS)	External — Inbound	DCPDS / DCHRMS	LC-02 (via LC-03)	Scheduled	Daily	HIGH	Raw: may contain PII (transient in-flight)
IF-02	Certification Data Ingestion (DLA TMS)	External — Inbound	DLA TMS	LC-02 (via LC-03)	Scheduled	Weekly	MEDIUM	Raw: Privacy Act-adjacent

Interface ID	Name	Type	Source	Destination	Trigger	Frequency	Dependency Risk	Data Classification
								(transient)
IF-03	Performance Data Ingestion (DPMAP)	External — Inbound	DPMAP	LC-02 (via LC-03)	Scheduled	Annual	MEDIUM	Aggregate only; CUI
IF-04	Workload Metrics Ingestion (EBS)	External — Inbound	EBS	LC-02 (via LC-03)	Scheduled	Weekly	MEDIUM	CUI; no PII
IF-05	Proxy Data Ingestion (OPM FWD)	External — Inbound	OPM FWD	LC-02	On-demand	As needed	LOW	Public dataset
IF-06	De-identified Records to Processed Zone	Internal — Outbound	LC-02	Processed Zone	Post-validation	Per ingestion cycle	N/A (internal)	CUI — de-identified
IF-07	Processed Zone to Ontology Update	Internal — Inbound	Processed Zone	LC-04	Post-ingestion	Per ingestion cycle	N/A	CUI — de-identified
IF-08	Processed Zone to Synthetic Engine	Internal — Inbound	Processed Zone	LC-05	Scheduled / on-demand	Per generation cycle	N/A	CUI — de-identified (training input)
IF-09	Synthetic Population to Synthetic Zone	Internal — Outbound	LC-05	Synthetic Zone	Post-validation	Per generation cycle	N/A	CUI — synthetic (pending PIA)
IF-10	Synthetic Population to Simulation Engine	Internal — Inbound	Synthetic Zone	LC-06	On scenario initiation	Per scenario run	N/A	CUI — synthetic
IF-11	Simulation Results to Analytical Zone	Internal — Outbound	LC-06	Analytical Zone	Post-simulation	Per scenario run	N/A	CUI
IF-12	Readiness Indicators to Decision Support	Internal — Bidirectional	LC-04 / Analytical Zone	LC-07	Continuous / on-demand	Per refresh + on-demand	N/A	CUI — no individual data

Interface ID	Name	Type	Source	Destination	Trigger	Frequency	Dependency Risk	Data Classification
IF-13	Alert Events to Alert Delivery	Internal — Outbound	LC-04	LC-11 (alert delivery)	Threshold crossing	Event-driven	N/A	CUI — no individual data
IF-14	Audit Events to Audit Log	Internal — Outbound (all services)	All ALICE services	LC-09	Every user and system event	Continuous	N/A	CUI — sensitive
IF-15	Synthetic Data Export Delivery	External — Outbound	LC-05	Authorized requester	Data Steward authorization	On-demand	N/A	CUI — synthetic (pending PIA)

3. Part A — External Integration Interfaces

External integration interfaces cross the ALICE system boundary. All external integrations are governed by ADR-009 (read-only enforcement at service account credential level). All inbound external flows carry the encryption requirements of REQ-SEC-006 (TLS 1.2+ in transit). All data use agreements required for DLA-specific integrations must be executed before any DLA data is ingested.

INT-01: DCPDS / DCHRMS Ingestion

Type: External — Inbound	**Direction**: Source to ALICE (inbound only; no write-back)	**Dependency Risk**: HIGH	**Phase**

Phase	I and II
External System	Defense Civilian Personnel Data System (DCPDS) in Phase I. Defense Civilian Human Resources Management System (DCHRMS) on migration per ADR-003.
Business Purpose	Provides ALICE with the authoritative record of DLA positions and de-identified person-position associations: occupational series, grade, duty station, fill status, supervisory indicators, and organizational assignment.
Data Exchanged	Position records (DE-01): Position ID, occupational series, grade, duty station, supervisory indicator, organizational assignment, required certifications. Person-Position Link source records (pre-de-identification for DE-03): to be de-identified at ingestion by LC-02. May contain Privacy Act-protected fields in transit. Phase I: de-identified extracts delivered by DLA (or confirmed de-identified by LC-02 on receipt). Phase II: read-only API delta feed.

Direction	Inbound to ALICE only. ADR-009 prohibits write-back under any circumstances.
Phase I Interface Type	Batch file exchange via encrypted, authenticated secure file transfer (SFTP or equivalent approved mechanism). ALICE initiates the pull on a defined schedule.
Phase II Interface Type	Synchronous read-only API delta query. ALICE calls the DCHRMS API with authenticated service account credentials and retrieves incremental updates since the last successful query. Batch file exchange remains an approved fallback for Phase II if live API access is unavailable.
Data Format	JSON, CSV, or XML per REQ-NF-014. Specific schema defined in the ALICE canonical data model specification (required Phase I design artifact). LC-03 translates DCPDS and DCHRMS native schemas to the canonical model.
Authentication and Authorization	Service account credentials with read-only scope, managed by LC-12. Data use agreement (Memorandum of Understanding) required before first data delivery per RL-21 and OQ-002. Certificate-based authentication preferred for Phase II API integration.
Frequency	Daily delta — ALICE ingests changes since the last successful extraction. Full refresh on first ingestion or after a gap exceeding a configurable threshold.
Error Handling	Source system unavailable: retry 3 times at 15-minute intervals. After third failure, escalate to System Administrator via LC-11 alert. Preserve prior twin state. Schema mismatch: log error with field details, abort ingestion for affected records, notify administrator. LC-03 schema deviation alert triggers. PII field detected in received extract: log PII rejection event, abort ingestion of affected record, notify administrator. Zero PII records written to Processed Zone.
Retry Behavior	3 retries at 15-minute intervals for connectivity failures. Schema and PII errors do not retry automatically; they require administrator review.
Availability Dependency	HIGH. DCPDS / DCHRMS unavailability stops data ingestion. Ontology and readiness indicators freeze at last successful refresh. OPM FWD proxy (INT-05) provides a fallback for Phase I if primary integration is delayed.
Data Classification	In transit: Privacy Act-protected records require CUI handling. At Processed Zone: CUI de-identified records after LC-02 transformation.
Audit and Logging	LC-09 audit events: ingestion job start, record counts received, schema validation result, PII rejection counts, completion status, and any failure events. All events include timestamp, data source identifier, and operator notifications sent.
Security Controls	TLS 1.2+ for all file transfer or API communication (REQ-SEC-006). Service account credentials stored in LC-12; rotated per System Security Plan schedule. Read-only service account scope enforced at DCPDS / DCHRMS access control list level (ADR-009). PII detection scan applied by LC-02 before any record is written to the Processed Zone.
Data Entities	DE-01 (Position); DE-03 (Person-Position Link, de-identified at ingestion).
Consuming Components	LC-03 (schema translation); LC-02 (de-identification and zone write).

Acceptance Criteria	Data loads successfully; canonical schema validates; zero PII fields in Processed Zone after ingestion; record counts logged; daily delta delivers within 24-hour data currency window.
Governing ADRs	ADR-003 (schema abstraction for DCPDS/DCHRMS migration); ADR-009 (read-only enforcement); ADR-006 (Phase I must use de-identified extracts before ATO)
Related PRD Requirements	REQ-F-001; REQ-F-006; REQ-INT-001; REQ-NF-001; REQ-NF-013; REQ-NF-014
Open Questions	[OPEN] OQ-002: Data use agreement must specify which party performs de-identification and how compliance is verified before delivery. [OPEN] OQ-004: DCHRMS migration schedule for pilot sub-component determines Phase I schema mapping scope in LC-03. [OPEN] ASM-004: DCHRMS migration assumed not to reach pilot sub-component during Phase I.

INT-02: DLA Training Management System Ingestion

Type: External — Inbound	**Direction**: Source to ALICE (inbound only; no write-back)	**Dependency Risk**: MEDIUM	**Phase**

Phase	I and II
External System	DLA Training Management System (DLA TMS).
Business Purpose	Provides ALICE with certification requirements and training completion records enabling computation of certification currency across the DLA workforce. Certification currency is a primary input to the ontology's readiness indicators and a key attribute in the synthetic population.
Data Exchanged	Certification definitions (DE-04): certification ID, name, issuing authority, expiration logic, applicable positions. Certification completion records (source for DE-05 after de-identification): completion dates, certification IDs, de-identified person-position references.
Direction	Inbound to ALICE only. No write-back to DLA TMS.
Phase I Interface Type	Batch file exchange via encrypted, authenticated secure file transfer. ALICE initiates the pull on a weekly schedule.
Phase II Interface Type	Read-only API or scheduled secure extract, depending on DLA TMS capability confirmed during Phase I integration planning.
Data Format	JSON, CSV, or XML per REQ-NF-014. Specific schema defined in the ALICE canonical data model specification. [OPEN] OQ-008: DLA TMS extract format must be confirmed with the system owner; non-standard formats require custom LC-03 schema mapping development.
Authentication and Authorization	Service account with read-only scope, managed by LC-12. DLA TMS system owner authorization required before service account can be provisioned.
Frequency	Weekly. Certification currency changes (completions, expirations) are less frequent than personnel data changes; weekly refresh is operationally adequate.
Error Handling	Same retry and escalation pattern as INT-01. Schema mismatch or PII detection aborts affected records, logs the event, and notifies the System Administrator.

Retry Behavior	3 retries at 15-minute intervals for connectivity failures. Schema and PII errors require administrator review before retry.
Availability Dependency	MEDIUM. DLA TMS unavailability prevents certification currency updates. Certification currency data from the prior week remains active. Degraded readiness indicator accuracy after one missed cycle; significant degradation after two or more missed cycles.
Data Classification	In transit: may contain Privacy Act-adjacent training records. At Processed Zone: CUI de-identified records (DE-04, DE-05).
Audit and Logging	LC-09 audit events: ingestion job start, record counts, schema validation result, PII scan result, completion status. Weekly cadence events are a normal operational log entry.
Security Controls	TLS 1.2+ in transit; read-only service account; PII detection scan by LC-02; service account credentials managed by LC-12.
Data Entities	DE-04 (Certification); DE-05 (Certification Currency Record, de-identified at ingestion).
Consuming Components	LC-03 (schema translation); LC-02 (de-identification and zone write).
Acceptance Criteria	Certification currency fields populated for all positions in pilot sub-component; training completion history importable; schema validated; zero PII records in Processed Zone.
Governing ADRs	ADR-009 (read-only enforcement); ADR-003 (schema abstraction in LC-03)
Related PRD Requirements	REQ-F-002; REQ-F-007; REQ-NF-013; REQ-NF-014
Open Questions	[OPEN] OQ-008: DLA TMS extract format and availability of a standard export must be confirmed with the DLA TMS system owner at Phase I kickoff. If non-standard, LC-03 schema mapping development adds scope to Phase I Month 2.

INT-03: DPMAP Performance Calibration Ingestion

Type: External — Inbound	**Direction**: Source to ALICE (inbound only; aggregate data only)	**Dependency Risk**: MEDIUM	**Phase**

Phase	I and II
External System	DPMAP (DoD Performance Management and Appraisal Program), delivered through the MyPerformance tool or the DCHRMS Performance Management module upon migration.
Business Purpose	Provides ALICE with aggregate performance tier distribution data by occupational series and grade band for use in productivity calibration within the organizational ontology and synthetic population generation. Performance data enables ALICE to model the distribution of workforce capability levels across occupational groups, improving the fidelity of simulation outputs.
Data Exchanged	Aggregate performance tier distributions only: percentage of workforce in each performance tier (e.g., outstanding, exceeds expectations, fully successful) by occupational series and grade band.

	No individual performance ratings. No record linking a specific de-identified or tokenized individual to a performance rating. This constraint is absolute and is governed by DoDI 1400.25, Vol. 431 (REQ-COMP-002; REQ-INT-003).
Direction	Inbound to ALICE only. No write-back to DPMAP.
Phase I Interface Type	Batch file exchange or secure structured query. Annual extract aligned to the DoD civilian performance rating cycle (typically July of each year for the prior annual cycle).
Phase II Interface Type	Same as Phase I. Annual frequency is driven by the DPMAP rating cycle, not by ALICE design; no benefit to higher-frequency integration.
Data Format	JSON, CSV, or XML aggregate summary format. Schema must explicitly prevent individual-record-level data from being included in any extract. [INFERRED] A data validation check in LC-02 must confirm that no individual-record fields are present in the received data before the extract is loaded.
Authentication and Authorization	Service account with read-only scope, managed by LC-12. DoDI 1400.25, Vol. 431 data use documentation must be completed and maintained in the governance record (REQ-COMP-002) before any DPMAP data is accessed.
Frequency	Annual, aligned to the DoD performance rating cycle.
Error Handling	Receipt of data containing individual performance records (not just aggregate distributions) must trigger immediate ingestion abort, PII rejection event logged to LC-09, and notification to System Administrator and DLA Privacy Officer. This is a compliance failure, not a routine error.
Availability Dependency	MEDIUM. Annual cycle means a missed extract has a 12-month impact on performance calibration data. ALICE continues to operate with prior-year calibration data; the impact on readiness indicator accuracy depends on workforce composition stability.
Data Classification	CUI. Aggregate performance distribution data does not contain individual records but remains CUI given its derivation from personnel performance data.
Audit and Logging	LC-09 audit events: extraction event with record structure validation result, data use documentation reference, aggregate statistics (occupational series and grade band count), and completion status.
Security Controls	TLS 1.2+ in transit; read-only service account; LC-02 data structure validation confirms aggregate-only format before zone write; data use documentation maintained in governance record.
Data Entities	Aggregate performance tier attribute within DE-03 (Person-Position Link).
Consuming Components	LC-03 (schema translation); LC-02 (validation and zone write).
Acceptance Criteria	Performance tier distribution data loaded; data use documentation reference present in governance record; no individual rating records present in ingested data; schema validated.
Governing ADRs	ADR-009 (read-only enforcement); ADR-002 (individual records excluded by zone architecture)
Related PRD Requirements	REQ-F-003; REQ-COMP-002; REQ-INT-003; REQ-NF-014
Open Questions	[INFERRED] The aggregate-only schema for the DPMAP extract must be

	formally defined in the data use agreement with DLA. The schema definition must make it technically impossible for individual records to appear in the extract format.

INT-04: EBS Workload Metrics Ingestion

Type: External — Inbound	**Direction**: Source to ALICE (inbound only; no write-back)	**Dependency Risk**: MEDIUM	**Phase**

Phase	I and II (conditional — EBS access not guaranteed in Phase I)
External System	DLA Enterprise Business System (EBS), SAP-based enterprise resource planning system supporting DLA logistics, supply chain, and financial operations.
Business Purpose	Provides ALICE with unit-level supply chain throughput metrics enabling correlation between workforce configuration and mission output. This data supports the mission-output linkage capability that distinguishes ALICE from conventional workforce analytics tools.
Data Exchanged	Unit-level throughput metrics (DE-06): organizational unit code, metric type (order fill rate, processing volume, on-time delivery rate), value, reporting period. No individual-level data. No financial detail below unit aggregation level.
Direction	Inbound to ALICE only. No write-back to EBS.
Phase I Interface Type	Batch file exchange or structured extract, if EBS access is authorized during Phase I. If EBS access is not available in Phase I, this interface is deferred and DE-06 data is absent from Phase I.
Phase II Interface Type	Batch file exchange or read-only API, depending on EBS system owner authorization and available extract mechanism.
Data Format	JSON, CSV, or XML per REQ-NF-014. Metric schema defined in the ALICE canonical data model specification.
Authentication and Authorization	Service account with read-only scope, managed by LC-12. EBS system owner authorization required — this authorization is separate from and additional to the general DLA data use agreement (OQ-007).
Frequency	Weekly. Throughput metrics are reported on weekly cycles aligned to DLA supply chain reporting periods.
Error Handling	Same retry and escalation pattern as INT-01. Anomalous metric values (outside the plausible range defined for each metric type) are flagged for administrator review before loading, per DE-06 data quality rules.
Availability Dependency	MEDIUM. EBS unavailability prevents workload metric updates. Mission-output correlation capability in LC-04 degrades. Core readiness monitoring (position fill, certification currency) is unaffected. Deferred entirely in Phase I if EBS authorization is not obtained.
Data Classification	CUI. No PII. Unit-level operational performance data.
Audit and Logging	LC-09 audit events: extraction event, record counts by organizational unit, anomaly detection results, completion status.
Security Controls	TLS 1.2+ in transit; read-only service account credentials in LC-12; anomaly detection in LC-02 before zone write.

Data Entities	DE-06 (Workload Metric).
Consuming Components	LC-03 (schema translation); LC-02 (validation and zone write).
Acceptance Criteria	Workload metrics mapped to organizational units; correlation calculable between staffing configuration and throughput metrics; schema validated.
Governing ADRs	ADR-009 (read-only enforcement)
Related PRD Requirements	REQ-F-004; REQ-NF-014
Open Questions	[OPEN] OQ-007: EBS access authorization may require a separate process beyond the general data use agreement. Must be confirmed with DLA GTPOC and EBS system owner at Phase I kickoff. If not available in Phase I, DE-06 is absent and mission-output correlation is deferred to Phase II.

INT-05: OPM Federal Workforce Data Proxy Pull

Type: External — Inbound	**Direction**: Source to ALICE (inbound; public dataset)	**Dependency Risk**: LOW	**Phase**

Phase	Phase I only (proxy path when DLA-specific data is unavailable)
External System	OPM Federal Workforce Data (FWD) platform at data.opm.gov. Launched January 2026. Contains EHRI-based federal workforce data back to FY2005.
Business Purpose	Provides a legally obtainable, publicly available federal workforce dataset for use as a Phase I proxy when DLA-specific DCPDS data is delayed by data use agreement execution timelines. Enables Phase I ontology construction, synthetic generation, and backtesting to proceed without being blocked by data sharing agreement delays.
Data Exchanged	EHRI status, dynamics, and payroll data: federal workforce position and personnel population data at the federal civilian workforce level. Not DLA-specific. Proxy flag must be set on all records derived from this dataset and all derived outputs must be labeled as proxy-sourced.
Direction	Inbound to ALICE only.
Phase I Interface Type	Public bulk download or public API. No authentication required (public dataset). ALICE retrieves the dataset on-demand when DLA-specific data is unavailable.
Phase II Interface Type	Not applicable. INT-01 replaces INT-05 when DLA-specific data becomes available. INT-05 is deactivated for Phase II operational deployment.
Data Format	Standard federal workforce data format published by OPM on data.opm.gov. LC-03 schema mapping for OPM FWD format is a required Phase I design artifact.
Authentication and Authorization	None required. Public dataset available without authentication.
Frequency	On-demand. Retrieved when DLA-specific data is not available. Not a scheduled recurring integration.
Error Handling	OPM FWD platform unavailability: retry with backoff. If unavailable for an

	extended period, log the failure and report to System Administrator. Phase I timeline may be affected if both INT-01 and INT-05 are unavailable simultaneously — this risk is documented in RISK-001.
Availability Dependency	LOW. Public dataset with no access barrier. Platform is managed by OPM; no ALICE-specific dependency on DLA infrastructure.
Data Classification	Public data at source. Within ALICE, all records derived from OPM FWD must be tagged with a proxy flag. Derived readiness indicators and simulation outputs based on proxy data must be labeled as proxy-sourced in all outputs presented to users.
Audit and Logging	LC-09 audit events: proxy data retrieval event with dataset version, record counts, and proxy flag confirmation.
Security Controls	Encrypted transport (TLS 1.2+) for the retrieval request even though the data is public, consistent with ALICE's baseline transport security posture.
Data Entities	DE-01 (Position, proxy-derived); DE-03 (Person-Position Link proxy, de-identified before zone write).
Consuming Components	LC-02 (validation, proxy flag assignment, zone write).
Acceptance Criteria	OPM FWD data ingested and validated; proxy flag set on all derived records; Phase I feasibility demonstration not blocked by DLA data access delays.
Governing ADRs	ADR-006 (Phase I proxy data enables compliance without ATO); ADR-009 (read-only; no write to OPM systems)
Related PRD Requirements	REQ-F-005; ASM-002 (fallback to OPM FWD if DLA data unavailable within 60 days of contract award)
Open Questions	[INFERRED] OPM FWD data format schema for the LC-03 canonical mapping must be developed during Phase I Month 1 to ensure readiness before DLA data decision timelines are known. [OPEN] OQ-010: The Phase I acceptance standard — whether proxy-based validation is accepted as evidence of ALICE architecture viability — must be confirmed with DLA GTPOC at Phase I kickoff.

INT-06: DoD PKI / CAC Authentication

Type: Identity Federation	**Direction**: DoD PKI Authority ↔ LC-01 / LC-08	**Dependency Risk**: HIGH	**Phase**

Phase	I and II
External System	DoD Public Key Infrastructure (PKI) Authority. Provides the trust anchor and certificate revocation service for Common Access Card (CAC) authentication.
Business Purpose	Enables multi-factor user authentication using the DoD Common Access Card as required by DoDI 8520.02 and REQ-SEC-001. This interface is the trust anchor for the entire ALICE identity and access control model: every user session is validated against the DoD PKI before any data access is granted.
Data Exchanged	Certificate validation requests (from LC-01 to DoD PKI): user certificate

	presented at login. Certificate validation responses (from DoD PKI to LC-01): valid/invalid, revocation status, certificate attributes. Authentication tokens: issued by LC-08 after successful PKI validation.
Direction	Bidirectional — LC-01 sends certificate validation requests; DoD PKI returns validation results.
Phase I Interface Type	PKI certificate validation. Standard DoD PKI integration using X.509 certificates and Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) for revocation checking. [OPEN] ASM-008: Feasibility of PKI integration in Phase I demonstration environment must be confirmed at contract award. If not available, an alternative MFA mechanism must be implemented as an interim measure.
Phase II Interface Type	Same as Phase I, with enhanced integration into the Phase II ZTA model (device trust, continuous session validation per ADR-004).
Data Format	X.509 digital certificate format. Standard DoD PKI certificate profile. Certificate validation responses per OCSP or CRL protocol.
Authentication and Authorization	This interface provides authentication rather than consuming it. LC-01 is the Policy Enforcement Point; LC-08 is the Policy Engine per ADR-004.
Frequency	Per user session. Certificate validation occurs at every session initiation. Certificate revocation status is checked at session initiation and on a configured re-validation interval during long sessions.
Error Handling	DoD PKI unavailable: LC-01 cannot validate new sessions. Existing authenticated sessions may continue until their tokens expire; new logins are blocked. LC-11 alert sent to System Administrator. Certificate invalid or revoked: login denied. LC-09 audit event logged with certificate identifier and denial reason. Certificate revocation check failure: conservative default is to deny login until revocation status can be confirmed. [INFERRED: This policy must be defined in the System Security Plan.]
Availability Dependency	HIGH. DoD PKI unavailability blocks all new user access. System-automated workflows (OW-1, OW-4) that do not require user session tokens continue unaffected during PKI outages.
Data Classification	Certificate metadata (identity information). Session credentials (transient). No workforce data is exchanged over this interface.
Audit and Logging	LC-09 audit events: every session initiation (success or failure), with certificate identifier, revocation check result, and user identity. Failed login attempts logged with source IP.
Security Controls	Encrypted transport (TLS 1.2+ minimum) for all PKI communication. Certificate revocation check required on every session initiation per NIST SP 800-53 IA-5. Authentication failure threshold monitoring by LC-11.
Data Entities	None (identity metadata only; no workforce data entities).
Consuming Components	LC-01 (Interface Control — authentication enforcement point); LC-08 (IAM — identity resolution and token issuance).
Acceptance Criteria	CAC authentication functional; certificate revocation check performed on each session initiation; unauthorized access (invalid certificate, revoked certificate) rejected and logged; authenticated users receive role-scoped tokens.
Governing ADRs	ADR-004 (identity-centric security — this interface is the foundation of the ZTA authentication model)

Related PRD Requirements	REQ-SEC-001 (MFA / CAC); DoDI 8520.02; NIST SP 800-53 IA-2
Open Questions	[OPEN] ASM-008 / RISK-004: CAC integration feasibility in Phase I demonstration environment must be confirmed at contract award. If not feasible, an alternative multi-factor authentication mechanism must be designed and documented as an interim Phase I measure with CAC targeted for Phase II.

4. Part B — Internal Information Flows

Internal information flows connect service components within the ALICE boundary. They do not cross the external system boundary except for IF-15 (Synthetic Data Export Delivery), which is outbound to an authorized external recipient. All internal flows use encrypted transport (TLS 1.2+ for in-transit inter-service calls; AES-256 or FIPS 140-3 equivalent for data at rest per REQ-SEC-006 and REQ-SEC-007). Authentication between services uses service identity credentials managed by LC-12 per ADR-004.

4.1 Ingestion Pipeline Flows (IF-01 through IF-09)

Information flows IF-01 through IF-05 correspond directly to external integrations INT-01 through INT-05 and represent the same data in transit from the source system to LC-03. The full specification for these flows is provided in Part A (INT-01 through INT-05). The following detail records cover IF-06 through IF-09, which are internal-only flows within the ingestion pipeline.

Flow	Name	Source	Destination	Data	Trigger	Security	Entities
IF-01	Source Data Ingestion	DCPDS / DCHRMS	LC-02 (via LC-03)	Position and person-position records (may contain PII in transit)	Scheduled daily	TLS 1.2+; service account; PII detection on receipt	DE-01, DE-03 (pre-de-identification)
IF-02	Certification Data Ingestion	DLA TMS	LC-02 (via LC-03)	Certification definitions and completion records (may contain PII in transit)	Scheduled weekly	TLS 1.2+; service account; PII detection on receipt	DE-04, DE-05 (pre-de-identification)
IF-03	Performance Data Ingestion	DPMAP	LC-02 (via LC-03)	Aggregate performance tier distributions only	Scheduled annually	TLS 1.2+; service account; aggregate-only schema validation	DE-03 (performance tier attribute)
IF-04	Workload Metrics Ingestion	EBS	LC-02 (via LC-03)	Unit-level throughput metrics	Scheduled weekly	TLS 1.2+; service account	DE-06

Flow	Name	Source	Destination	Data	Trigger	Security	Entities
IF-05	Proxy Data Ingestion	OPM FWD	LC-02	EHRI workforce data (public)	On-demand	TLS 1.2+; no auth required (public)	DE-01, DE-03 (proxy-derived)

IF-06: De-identified Records to Processed Zone

Source	LC-02 (Data Ingestion and De-Identification Service)
Destination	Processed Zone (Zone 2)
Data Exchanged	De-identified position records (DE-01), person-position link records (DE-03), certification definitions (DE-04), certification currency records (DE-05), workload metrics (DE-06). All fields validated and de-identified before this flow. No Privacy Act records.
Trigger	Immediately after successful schema validation and PII scan confirmation for each ingestion batch.
Direction	Outbound from LC-02 to Processed Zone.
Transport Requirement	Encrypted write to the Processed Zone storage. AES-256 or FIPS 140-3 equivalent at rest (REQ-SEC-007). Access credentials for the Processed Zone are held only by LC-02; no other service has write credentials to this zone.
Validation Requirements	Schema validation must pass. PII scan must confirm zero PII fields. Both conditions must be confirmed before any record is written. If either fails, the affected record is rejected and logged; validated records may proceed.
Transformation Requirements	De-identification has been applied upstream. No additional transformation at this boundary except application of the zone encryption.
Error Handling	Write failure (storage unavailable): retry with exponential backoff. Alert LC-11 after configurable failure threshold. Preserve in-flight records in a durable queue; do not discard validated records on transient write failure.
Retry Behavior	Exponential backoff for transient storage failures. No retry on schema or PII validation failures — those require administrator review.
Audit Requirements	LC-09 event: zone write completion with record counts by entity type, zone write timestamp, batch identifier, and validation confirmation.
Privacy Considerations	This flow is the point at which de-identified records first enter persistent ALICE storage. Correctness of the de-identification transformation at this point is the primary Privacy Act compliance control. Any record containing a PII field that reaches this flow is a compliance failure requiring immediate investigation.
Data Entities	DE-01, DE-03, DE-04, DE-05, DE-06
Governing ADRs	ADR-002 (LC-02 is sole writer to Processed Zone); ADR-009 (read-only ingestion from source — no write-back implied by this internal flow)
Related Requirements	REQ-F-001 through REQ-F-006; REQ-NF-013; REQ-SEC-006; REQ-SEC-007

IF-07: Processed Zone to Ontology Update

Source	Processed Zone (Zone 2)
Destination	LC-04 (Organizational Ontology and Twin State Service)
Data Exchanged	De-identified position records (DE-01), role data (DE-02, if applicable), person-position links (DE-03), certification definitions (DE-04), certification currency records (DE-05), workload metrics (DE-06). CUI.
Trigger	Ingestion completion signal from LC-02 after successful zone write.
Direction	Inbound to LC-04 (read from Processed Zone).
Transport Requirement	Encrypted at-rest access to Processed Zone storage. LC-04 read credentials managed by LC-12.
Validation Requirements	LC-04 validates referential integrity (position IDs referenced in person-position links must exist in position records; certification IDs referenced in currency records must exist in certification definitions).
Transformation Requirements	LC-04 constructs and updates the organizational ontology graph from the de-identified records. This transformation is internal to LC-04 and involves role assignment, dependency graph construction, and readiness indicator computation.
Error Handling	If Processed Zone is unavailable when LC-04 attempts to read: retry with backoff; alert LC-11; retain prior ontology state until successful refresh.
Audit Requirements	LC-09 event: ontology update completion with record counts processed, readiness indicator recomputation status, historical snapshot creation timestamp.
Privacy Considerations	LC-04 reads de-identified records only. No Privacy Act records exist in the Processed Zone by design. Activity-scope enforcement is applied within LC-04 at query time.
Data Entities	DE-01, DE-02, DE-03, DE-04, DE-05, DE-06 (reads); DE-07 (produces Readiness Indicators as output in Analytical Zone)
Governing ADRs	ADR-002 (LC-04 reads Processed Zone; writes Analytical Zone)
Related Requirements	REQ-F-007; REQ-F-008; REQ-F-009; REQ-NF-001

IF-08: Processed Zone to Synthetic Engine (Training Input)

Source	Processed Zone (Zone 2)
Destination	LC-05 (Synthetic Workforce Engine Service) — generative model training environment
Data Exchanged	De-identified person-position links (DE-03) and certification currency records (DE-05). CUI. This is the training corpus for the generative model.
Trigger	Scheduled generation cycle or on-demand System Administrator trigger.
Direction	Inbound to LC-05 training environment (read from Processed Zone).
Transport Requirement	Encrypted at-rest access to Processed Zone. LC-05 training environment read credentials managed by LC-12. The training environment must be isolated from LC-06 and LC-07 at the network and credential level.
Validation Requirements	Record count confirmed before training begins. If record count is below the minimum viable training corpus size (ASM-003: 300 positions), training is blocked and the System Administrator is notified.

Transformation Requirements	The generative model training process applies differential privacy noise injection during training (epsilon ≤ 1.0). The training input records are used only within the training environment; they are not persisted in the LC-05 service after training completes.
Error Handling	Training environment unavailable: defer generation cycle; alert LC-11. Training corpus below minimum size: block generation; notify administrator; log event.
Audit Requirements	LC-09 event: generation cycle initiation with source dataset version identifier, record counts, and training environment confirmation.
Privacy Considerations	De-identified records from the Processed Zone are the training input. They must not persist in the LC-05 application context after training completes. The generative model parameters (not the raw records) are the persisted output. Training environment isolation from simulation and decision support services is the key control.
Data Entities	DE-03, DE-05 (training inputs); DE-08 (produced in Synthetic Zone); DE-12 (generation metadata produced concurrently)
Governing ADRs	ADR-002 (LC-05 reads Processed Zone, writes Synthetic Zone); ADR-007 (training input is de-identified CUI; output is CUI synthetic)
Related Requirements	REQ-F-015; REQ-F-016; REQ-F-017; REQ-NF-005

IF-09: Synthetic Population to Synthetic Zone

Source	LC-05 (Synthetic Workforce Engine — after validation)
Destination	Synthetic Zone (Zone 3)
Data Exchanged	Validated synthetic population (DE-08) and generation metadata (DE-12). CUI by default pending PIA (ADR-007).
Trigger	Immediately after both fidelity validation (KS test, chi-squared; target ≤ 5% deviation) and privacy validation (membership inference attack; target ≤ 50% success rate) pass.
Direction	Outbound from LC-05 to Synthetic Zone.
Transport Requirement	Encrypted write to Synthetic Zone storage. AES-256 or FIPS 140-3 equivalent at rest. LC-05 write credentials to Synthetic Zone managed by LC-12. Promotion is atomic: if either validation failed, no write to Synthetic Zone occurs.
Validation Requirements	Both fidelity and privacy validations must pass before this flow executes. Validation results documented in DE-12 before zone write. Failed generations result in quarantine, not zone write.
Transformation Requirements	None. The synthetic population is promoted as-is from the training environment output to the Synthetic Zone.
Error Handling	Zone write failure on a validated population: retry with exponential backoff. Log the failure. Preserve the prior validated population as active until write succeeds.
Audit Requirements	LC-09 event: synthetic population promotion with DE-12 reference, fidelity result summary, privacy result summary, population record count, epsilon applied, zone write timestamp.
Privacy Considerations	This flow promotes data that is CUI by default (ADR-007). CUI marking applied at write. No individual real-person data exists in this flow by

	design.
Data Entities	DE-08 (Synthetic Person — written); DE-12 (Generation Metadata — written concurrently)
Governing ADRs	ADR-002 (LC-05 is sole writer to Synthetic Zone); ADR-007 (CUI by default)
Related Requirements	REQ-F-015; REQ-F-016; REQ-F-017; REQ-NF-005

4.2 Simulation and Decision Support Flows (IF-10 through IF-13)

IF-10: Synthetic Population to Simulation Engine

Source	Synthetic Zone (Zone 3)
Destination	LC-06 (Agent-Based Simulation Engine)
Data Exchanged	Current validated synthetic population (DE-08). CUI synthetic.
Trigger	User-initiated scenario execution request received by LC-06 from LC-07.
Direction	Inbound to LC-06 (read from Synthetic Zone).
Transport Requirement	Encrypted at-rest read from Synthetic Zone. LC-06 read credentials to Synthetic Zone only — no Processed Zone credentials (ADR-008). Access credentials managed by LC-12.
Validation Requirements	LC-06 confirms that the synthetic population is current (not expired per the configured expiration policy). If population is expired, LC-06 returns an error to LC-07 and the scenario is blocked pending regeneration.
Transformation Requirements	LC-06 instantiates agents from synthetic population attributes. The synthetic records serve as the population from which agents are drawn; they are held in the simulation execution context only and are not persisted by LC-06.
Error Handling	Population expired: block scenario; notify user via LC-07 with regeneration required message; log event to LC-09. Synthetic Zone unavailable: block scenario; alert LC-11.
Audit Requirements	LC-09 event: synthetic population read for simulation, with synthetic population version reference, scenario run ID, and record count.
Privacy Considerations	LC-06 reads only from the Synthetic Zone. No access to Processed Zone (ADR-008). Synthetic records are not records of real individuals. No Privacy Act risk in this flow.
Data Entities	DE-08 (read for simulation); DE-09 (produced by LC-06 in Analytical Zone after simulation)
Governing ADRs	ADR-002 (Synthetic Zone read); ADR-008 (LC-06 restricted to Synthetic Zone — no Processed Zone access)
Related Requirements	REQ-F-010; REQ-F-012; REQ-F-013; REQ-NF-002

IF-11: Simulation Results to Analytical Zone

Source	LC-06 (Agent-Based Simulation Engine)
Destination	Analytical Zone (Zone 4)

Data Exchanged	Scenario run results (DE-09 record and associated output files): time-series readiness forecast, confidence intervals, at-risk position list, response option comparison. CUI.
Trigger	Immediately after simulation execution and results computation complete.
Direction	Outbound from LC-06 to Analytical Zone.
Transport Requirement	Encrypted write to Analytical Zone. AES-256 or FIPS 140-3 equivalent at rest. LC-06 write credentials to Analytical Zone managed by LC-12.
Validation Requirements	Results structure validated against the defined output schema before zone write. Confidence intervals must be present on all forecast outputs (REQ-F-014). If confidence interval generation failed, results are flagged before write.
Transformation Requirements	Results are formatted into the defined structured output schema (time-series readiness forecast, at-risk position list, response option comparison table) before zone write.
Error Handling	Zone write failure: retry with backoff. Results are preserved in-flight until write succeeds. If write ultimately fails, scenario run is marked as failed in the audit log; user is notified.
Audit Requirements	LC-09 event: scenario run record creation in Analytical Zone, with run ID, user ID, scenario type, duration, and output file reference.
Privacy Considerations	Results contain no individual-identifiable data. Results represent aggregate population-level simulation outcomes. CUI classification applies.
Data Entities	DE-09 (Scenario Run — created in Analytical Zone)
Governing ADRs	ADR-002 (LC-06 writes Analytical Zone)
Related Requirements	REQ-F-012; REQ-F-014; REQ-F-023

IF-12: Readiness Indicators to Decision Support Interface

Source	LC-04 (Ontology Service) and Analytical Zone (Zone 4)
Destination	LC-07 (Decision Support Interface)
Data Exchanged	Readiness indicators (DE-07), position risk register data (DE-01 attributes), historical state snapshots for trend view, alert notifications. All CUI. All role-scoped and activity-scoped.
Trigger	Continuous (updated on each ingestion cycle for dashboards); on-demand (user data requests and scenario result queries).
Direction	Inbound to LC-07 (read from LC-04 and Analytical Zone). Outbound from LC-07 to LC-06 for scenario initiation requests (handled as a separate sub-flow).
Transport Requirement	TLS 1.2+ for all LC-04 to LC-07 service calls. Role-scoped access token from LC-01 validated at LC-04 before any data is returned.
Validation Requirements	Role and activity scope must be validated by LC-04 before any data is returned to LC-07. LC-07 must not receive data for activities outside the requesting user's authorized scope.
Transformation Requirements	LC-04 applies activity-scope filtering at the query layer. LC-07 renders the returned data according to role-appropriate view templates.
Error Handling	LC-04 unavailable: LC-07 displays a data unavailability notice with the

	timestamp of the last successful refresh. Stale data is not silently displayed as current. Data currency timestamp (REQ-UX-008) enables users to assess staleness.
Audit Requirements	LC-09 event: user data access event for each readiness indicator query, with user ID, scope accessed, data type, and timestamp.
Privacy Considerations	All data returned is de-identified and aggregate. Activity scope enforcement at LC-04 prevents cross-activity data access. No individual-identifying data is present in any output of this flow.
Data Entities	DE-07 (Readiness Indicator); DE-01 (Position attributes for risk register); DE-09 (Scenario Run results for historical view)
Governing ADRs	ADR-002 (Analytical Zone read by LC-07); ADR-004 (role-scoped token required for every request)
Related Requirements	REQ-F-009; REQ-F-019; REQ-F-020; REQ-F-021; REQ-UX-001; REQ-UX-005; REQ-UX-008

IF-13: Alert Events to Alert Delivery

Source	LC-04 (Ontology Service — threshold evaluation)
Destination	LC-11 (Observability and Health Monitoring) for delivery to designated System Administrator; LC-07 (Decision Support Interface) for user-facing alert display.
Data Exchanged	Threshold crossing event notifications: affected mission function area, severity level, current indicator value, threshold value, timestamp. CUI. No individual-identifying data.
Trigger	When LC-04 determines that a readiness indicator has crossed a configured threshold value during ontology refresh.
Direction	Outbound from LC-04 to LC-11 (operational alert) and LC-07 (user notification queue).
Transport Requirement	Internal encrypted service-to-service communication (TLS 1.2+ for inter-service calls). LC-07 displays alerts on next user login if not previously acknowledged (REQ-UX-003).
Validation Requirements	Alert events must include all required fields (function area, severity, threshold, current value, timestamp) before delivery. Incomplete alert events must be logged as malformed and not delivered silently.
Transformation Requirements	LC-07 formats alert events for role-appropriate display: enterprise-level alerts visible to Enterprise Decision-Maker role; activity-scoped alerts visible to Activity Directors for their assigned activity only.
Error Handling	Delivery failure to LC-07: alert queued for next user login. Delivery failure to LC-11: log the failure to LC-09; System Administrator is responsible for checking LC-09 directly in this scenario.
Audit Requirements	LC-09 event: alert generation with function area, severity, indicator value, threshold, and delivery confirmation.
Privacy Considerations	Alert events reference organizational function areas and readiness scores. No individual data. CUI classification applies.
Data Entities	DE-07 (Readiness Indicator — source of threshold crossing event)
Governing ADRs	ADR-010 (threshold values are configuration-driven per LC-10)

Related Requirements	REQ-F-022; REQ-UX-003

4.3 Governance and Audit Flows (IF-14 through IF-15)

IF-14: Audit Events to Audit Log

Source	All ALICE service components (LC-01 through LC-12)
Destination	LC-09 (Immutable Audit Logging Service)
Data Exchanged	Structured audit event records per the minimum audit event catalog defined in SDP-ART-02 Section 3.5. CUI — sensitive. Events include: user and system actions, data access events, zone boundary crossings, configuration changes, ingestion events, generation events, export events, alert events, and authentication events.
Trigger	On every user action, system event, data transformation, zone boundary crossing, and access attempt. Continuous and event-driven.
Direction	Outbound from all services (write-only) to LC-09.
Transport Requirement	Encrypted inter-service communication. Write-only delivery interface — services can append events but cannot read or modify existing log entries. Durable event queue in LC-09 to absorb bursts and survive transient storage unavailability.
Validation Requirements	Each event must contain: entry ID (assigned by LC-09), UTC timestamp, actor identity, action type (from defined enumeration), affected entity reference, outcome, and source identifier. Events missing required fields are logged as malformed audit events and flagged for administrator review — they are not silently discarded.
Transformation Requirements	LC-09 appends an integrity hash on receipt. The hash chain enables tamper detection for the complete log sequence.
Error Handling	LC-09 unavailable: services buffer events in a durable local queue and deliver when connectivity is restored. Event loss due to LC-09 permanent unavailability is a critical security incident. Services must not suppress event generation during LC-09 downtime.
Retry Behavior	Buffered retry until delivery confirmed. No TTL-based discard of audit events during transient LC-09 unavailability.
Audit Requirements	This flow is itself part of the audit architecture. The intake of audit events by LC-09 is the final step in the chain; no secondary audit is required for the IF-14 flow itself.
Privacy Considerations	Audit log entries reference user identities and event metadata but must not contain raw workforce data content (e.g., position salary data or individual performance ratings). References to entity IDs are permitted; entity attribute values are not.
Data Entities	DE-11 (Audit Log Entry — created by this flow)
Governing ADRs	ADR-005 (dedicated immutable audit service — this flow implements the ADR)
Related Requirements	REQ-NF-012; REQ-SEC-009; REQ-SEC-010; NIST SP 800-53 AU-2, AU-3, AU-9, AU-11

IF-15: Synthetic Data Export Delivery

Source	LC-05 (Synthetic Workforce Engine — export function)
Destination	Authorized external requester (may be internal DLA analyst or authorized external partner depending on the approved use case)
Data Exchanged	Validated synthetic population export file (DE-08 subset as requested) with provenance metadata including: synthetic population version, epsilon applied, fidelity test results, generation timestamp, Data Steward authorization reference, export file cryptographic hash.
Trigger	Data Steward approval of a synthetic data export request (OW-3 completion). Export does not occur before Steward authorization is confirmed.
Direction	Outbound from ALICE to authorized external recipient. This is the only outbound data flow that crosses the ALICE system boundary to a non-ALICE recipient.
Transport Requirement	Encrypted authorized channel. The specific channel must be an approved secure transfer mechanism appropriate for CUI data exchange (TLS 1.2+ encrypted transfer or equivalent government-approved mechanism). The channel must be confirmed as CUI-capable before delivery.
Validation Requirements	Current synthetic population must be validated (fidelity and privacy tests passed; population not expired). Steward authorization must be confirmed before export file is generated. Export file hash must be computed and attached before delivery.
Transformation Requirements	LC-05 generates the export file from the current validated synthetic population with the requested attribute set and attaches provenance metadata.
Error Handling	Delivery failure to requester: notify requester; notify Data Steward; log delivery failure event to LC-09. Do not retry delivery to an unconfirmed recipient channel without Steward re-authorization.
Retry Behavior	No automatic retry to external recipient. Delivery must be re-initiated with Steward re-authorization if the initial delivery fails.
Audit Requirements	LC-09 immutable event (DE-10): export ID, requester ID, use case, Steward ID, authorization decision, timestamp, export file hash, delivery method, and delivery confirmation. Non-deletable.
Privacy Considerations	Export file is CUI by default pending PIA determination (ADR-007). Recipients must be cleared to handle CUI. Export files carry CUI markings. The provenance metadata attached to each export enables after-the-fact traceability of any derived analytical product back to its ALICE generation event.
Data Entities	DE-08 (Synthetic Person — exported); DE-10 (Synthetic Data Export — governance record created); DE-12 (Generation Metadata — referenced in provenance)
Governing ADRs	ADR-007 (CUI by default); ADR-005 (immutable export log entry required); ADR-002 (export authorized only from Synthetic Zone)
Related Requirements	REQ-F-018; REQ-NF-008; REQ-COMP-001; REQ-COMP-004

5. Part C — Cross-Reference Tables

5.1 Interface to Component Mapping

Interface	Producing Component	Consuming Component(s)	Zone Boundary Crossed?
INT-01 / IF-01	External DCPDS/DCHRMS	LC-03 → LC-02	Yes (external to ALICE)
INT-02 / IF-02	External DLA TMS	LC-03 → LC-02	Yes (external to ALICE)
INT-03 / IF-03	External DPMAP	LC-03 → LC-02	Yes (external to ALICE)
INT-04 / IF-04	External EBS	LC-03 → LC-02	Yes (external to ALICE)
INT-05 / IF-05	External OPM FWD	LC-02	Yes (public internet to ALICE)
INT-06	External DoD PKI	LC-01, LC-08	Yes (DoD identity zone to ALICE)
IF-06	LC-02	Processed Zone	Yes (zone boundary: Raw → Processed)
IF-07	Processed Zone	LC-04	Yes (zone boundary: Processed → LC-04)
IF-08	Processed Zone	LC-05 (training env)	Yes (zone boundary: Processed → LC-05 training)
IF-09	LC-05	Synthetic Zone	Yes (zone boundary: LC-05 → Synthetic)
IF-10	Synthetic Zone	LC-06	Yes (zone boundary: Synthetic → LC-06)
IF-11	LC-06	Analytical Zone	Yes (zone boundary: LC-06 → Analytical)
IF-12	LC-04, Analytical Zone	LC-07	No (internal; scope-enforced query)
IF-13	LC-04	LC-11, LC-07	No (internal service-to-service)
IF-14	All services	LC-09	No (internal; all services write to LC-09)
IF-15	LC-05 (export)	External authorized requester	Yes (ALICE boundary to external recipient)

5.2 Interface to Data Entity Mapping

Interface	Data Entities Involved	Classification In Transit	Classification at Rest
INT-01 / IF-01	DE-01 (in transit), DE-03 (pre-de-identification in transit)	Privacy Act-protected in transit	CUI (de-identified) in Processed Zone
INT-02 / IF-02	DE-04 (in transit), DE-05 (pre-de-identification)	Privacy Act-adjacent in transit	CUI (de-identified) in Processed Zone

Interface	Data Entities Involved	Classification In Transit	Classification at Rest
INT-03 / IF-03	DE-03 (performance tier attribute only — aggregate)	CUI	CUI in Processed Zone
INT-04 / IF-04	DE-06	CUI	CUI in Processed Zone
INT-05 / IF-05	DE-01, DE-03 (proxy-derived)	Public	CUI (proxy-flagged) in Processed Zone
INT-06	Identity metadata only (no DE entities)	N/A — credential metadata	N/A — transient
IF-06	DE-01, DE-03, DE-04, DE-05, DE-06	CUI (de-identified)	CUI in Processed Zone
IF-07	DE-01, DE-02, DE-03, DE-04, DE-05, DE-06	CUI	CUI in Processed Zone
IF-08	DE-03, DE-05 (training input); DE-08 (produced); DE-12 (produced)	CUI	CUI in Synthetic Zone
IF-09	DE-08, DE-12	CUI	CUI in Synthetic Zone (pending PIA)
IF-10	DE-08 (read for simulation)	CUI	CUI in Synthetic Zone
IF-11	DE-09 (scenario run results)	CUI	CUI in Analytical Zone
IF-12	DE-07, DE-01 (attributes), DE-09 (historical)	CUI	CUI in Analytical Zone
IF-13	DE-07 (alert trigger source)	CUI	CUI in Analytical Zone
IF-14	DE-11 (Audit Log Entry — created)	CUI — sensitive	CUI in Audit Log Store
IF-15	DE-08 (export), DE-10 (governance record), DE-12 (provenance reference)	CUI	CUI at rest; CUI in transit to authorized recipient

5.3 Interface to PRD Requirement Mapping

Interface	Primary PRD Requirements	Governing ADRs	Risk Level
INT-01 / IF-01	REQ-F-001; REQ-F-006; REQ-INT-001; REQ-NF-001; REQ-NF-013; REQ-NF-014	ADR-003; ADR-009; ADR-006	HIGH — schema migration risk; data use agreement dependency
INT-02 / IF-02	REQ-F-002; REQ-F-007; REQ-NF-013; REQ-NF-014	ADR-003; ADR-009	MEDIUM — extract format uncertainty
INT-03 / IF-03	REQ-F-003; REQ-COMP-002; REQ-INT-003; REQ-NF-014	ADR-009	MEDIUM — aggregate-only constraint must be enforced in data use agreement

Interface	Primary PRD Requirements	Governing ADRs	Risk Level
INT-04 / IF-04	REQ-F-004; REQ-NF-014	ADR-009	MEDIUM — separate EBS authorization required
INT-05 / IF-05	REQ-F-005; ASM-002	ADR-006; ADR-009	LOW — public dataset; fallback path
INT-06	REQ-SEC-001; DoDI 8520.02	ADR-004	HIGH — blocks all user access if unavailable
IF-06	REQ-F-001 through REQ-F-006; REQ-NF-013; REQ-SEC-006; REQ-SEC-007	ADR-002; ADR-009	N/A (internal — risk inherited from INT-01 through INT-05)
IF-07	REQ-F-007; REQ-F-008; REQ-F-009; REQ-NF-001	ADR-002	N/A (internal)
IF-08	REQ-F-015; REQ-F-016; REQ-F-017; REQ-NF-005	ADR-002; ADR-007	N/A (internal)
IF-09	REQ-F-015; REQ-F-016; REQ-F-017; REQ-NF-005	ADR-002; ADR-007	N/A (internal)
IF-10	REQ-F-010; REQ-F-012; REQ-F-013; REQ-NF-002	ADR-002; ADR-008	N/A (internal)
IF-11	REQ-F-012; REQ-F-014; REQ-F-023	ADR-002	N/A (internal)
IF-12	REQ-F-009; REQ-F-019; REQ-F-020; REQ-F-021; REQ-UX-001; REQ-UX-008	ADR-002; ADR-004	N/A (internal)
IF-13	REQ-F-022; REQ-UX-003	ADR-010	N/A (internal)
IF-14	REQ-NF-012; REQ-SEC-009; REQ-SEC-010; REQ-F-018	ADR-005	N/A (internal — critical compliance flow)
IF-15	REQ-F-018; REQ-NF-008; REQ-COMP-001; REQ-COMP-004	ADR-007; ADR-005; ADR-002	MEDIUM — outbound CUI; Steward authorization required

6. Interface Governance Rules

The following rules govern all ALICE interfaces. They are Source-Derived from PRD Section 19 (Integration Requirements) and TNA Section 14.3 (Integration Constraints) and apply to all interfaces documented in this catalog.

Rule ID	Rule Statement	Source	Validation Method
IGR-01	All external source system integrations are read-only. No write, modify, or delete interface to any source system shall be implemented at any point in Phase I or Phase II.	ADR-009; CON-002; CON-004; PRD Section 11.2	Penetration test: confirm zero write capability on source system service accounts. Code review of LC-02 and LC-03: confirm no write operations to external systems.

Rule ID	Rule Statement	Source	Validation Method
IGR-02	Data use agreements must be executed before any DLA-specific workforce data (DE-01 through DE-06 from DLA sources) is ingested. OPM FWD proxy data (INT-05) may be used before agreement execution.	DGR-05; ADR-006; PRD Section 4.4	DUA execution record maintained in governance record. No DLA-specific data ingestion event in LC-09 before DUA execution date.
IGR-03	Integration service account credentials shall be managed through LC-12 and rotated on the schedule defined in the System Security Plan. No credential shall be stored in configuration files, environment variables, or application code.	REQ-SEC-008; ADR-004	Secrets audit: confirm all source system credentials reside in LC-12. Code review: confirm no hardcoded credentials in LC-02 or LC-03.
IGR-04	The schema abstraction layer (LC-03) must support both DCPDS and DCHRMS schemas without requiring redeployment of any other ALICE service component.	ADR-003; REQ-INT-001	Schema migration test: update LC-03 DCHRMS mapping; confirm LC-02, LC-04, LC-05, and LC-06 continue to operate without code changes.
IGR-05	All integration interfaces shall use standard data exchange formats (JSON, CSV, or XML). Proprietary or vendor-specific binary formats shall not be used for primary integration interfaces.	REQ-NF-014; AP-9 (Open Standards)	Integration test: confirm all interface outputs are parseable by standard open-source parsers without proprietary client libraries.
IGR-06	All external interfaces crossing the ALICE system boundary shall use TLS 1.2 or higher for transport encryption.	REQ-SEC-006; NIST SP 800-53 SC-8	Security assessment: TLS version verification on all external connections. Automated scan of interface endpoints.
IGR-07	The synthetic data export interface (IF-15) shall not deliver any export file before an immutable DE-10 governance record has been created in LC-09.	REQ-F-018; DGR-06; ADR-005	Audit review: confirm every delivery event in LC-11 has a corresponding DE-10 record created before the delivery timestamp.

7. Gate-5 Summary and Decision Required

What Was Created

Artifact 5 (Interface Catalog) documents all 21 ALICE interfaces — six external integration interfaces (INT-01 through INT-06) and fifteen internal information flows (IF-01 through IF-15) — in a three-part structure. Part A provides full specifications for each external integration interface including interface type by phase, authentication method, data format, error handling, retry behavior, audit requirements, security controls, data entity mapping, acceptance criteria, and governing ADRs. Part B provides full specifications for all fifteen internal information flows, with detailed records for the architecturally critical flows (IF-06 through IF-15) and a summary table for IF-01 through IF-05, which duplicate the external integration detail already covered in Part A. Part C provides three cross-reference tables mapping interfaces to components, data entities, and PRD requirements. Section 6 establishes seven Interface Governance Rules (IGR-01 through IGR-07) governing all interfaces in the catalog.

Major Assumptions

- INT-01 (DCPDS/DCHRMS): both schemas are addressable by LC-03 per ADR-003. DCHRMS migration timing for the pilot sub-component is unknown; ASM-004 assumes migration does not reach the pilot sub-component during Phase I.
- INT-06 (CAC): CAC integration in the Phase I demonstration environment is an assumption per ASM-008. If not available, an alternative MFA mechanism must be designed as an interim Phase I measure.
- INT-04 (EBS): EBS access is conditional; if separate authorization is not obtained before Phase I demonstration, DE-06 data and mission-output correlation are deferred.
- IF-13 (Alert Delivery): the alert delivery mechanism (in-system notification vs. email vs. both) is not explicitly specified in the PRD. The catalog treats this as a configurable delivery capability per ADR-010. The delivery mechanism must be specified before Phase II design.

Open Issues

- **[Critical]** OQ-002: Data use agreement must specify which party de-identifies DCPDS/DCHRMS data before delivery. This directly affects INT-01 and IF-01 design.
- **[High]** ASM-008 / RISK-004: CAC integration feasibility for INT-06 in Phase I must be confirmed at contract award.
- **[High]** OQ-007: EBS system owner authorization for INT-04 must be confirmed. If not available in Phase I, INT-04 / IF-04 are deferred.
- **[Medium]** OQ-008: DLA TMS extract format must be confirmed for INT-02 schema mapping in LC-03.
- **[Medium — Inferred]** Alert delivery mechanism for IF-13 (in-system vs. email vs. push notification) must be specified before Phase II interface design. This is a configurable parameter per ADR-010 but must be defined for the System Security Plan.
- **[Medium — Inferred]** DPMAP aggregate-only schema (INT-03) must be formally defined in the data use agreement to technically prevent individual records from being included in the extract. This design task requires DLA HRMS and DPMAP system owner coordination.

Decision Required

Gate-5 Decision: Please approve Artifact 5 (Interface Catalog) to proceed to Artifact 6 (Risk Register), or provide specific revision instructions. If any interface specification — including interface type, authentication method, error handling behavior, audit requirement, or acceptance criteria — requires modification, please identify the interface ID (INT-XX or IF-XX) and the specific

change required. Interface Governance Rules (IGR-01 through IGR-07) are also subject to stakeholder revision at this gate.