

FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD

Version 2.2 Formal Conformance Test Suite, CF-01 through CF-79

Verified assessor-facing consolidated reader edition | 12 September 2026

CONTROLLED STATUS AND SOURCE METHOD

This edition supersedes the provisional Version 2.2 consolidated suite for reader-facing assessor use. It restores source-specific control language for CF-01 through CF-69 from the Version 2.1 development record, then incorporates adopted CF-70 through CF-78 and adopted IR-01 CF-79. No standardized generic procedure is substituted where source-specific language exists.

CF-01 through CF-40 derive from the Version 2.1-RC1 Formal Conformance Specification. CF-41 through CF-69 derive from later controlled development blocks incorporated before the Version 2.1 freeze. CF-70 through CF-78 derive from the Version 2.2 SD-01 Normative Traceability and Conformance Extension. CF-79 derives from the adopted IR-01 controlled extension.

ASSESSMENT RULE

Conformance is based on actual governmental informational capability and evidence, not policy assertions alone.

CF-01 — Actor Enumeration

Requirement

The system SHALL identify all categories of actors capable of exercising informational power.

Evidence

Actor and role inventory.

Test

Determine whether the inventory includes:

ordinary users;

supervisors;

investigators;

administrators;

developers;

contractors;

vendors;

AI agents;

service accounts;

auditors;

external government entities.

PASS

All materially capable actors are identified.

FAIL

Material actors or machine identities are omitted.

XI. INFORMATION DOMAIN REQUIREMENTS

CF-02 — Information Domain Identification

Requirement

Information SHALL be categorized into meaningful governmental purpose domains.

Evidence

Data inventory and functional mappings.

Test

Ask whether information can be associated with identifiable governmental functions rather than merely technical repositories.

PASS

Domains correspond to identifiable governmental purposes.

FAIL

The architecture treats all individualized information as a common undifferentiated resource.

XII. ORIGINATING INFORMATIONAL PURPOSE

CF-03 — OIP Identification

Requirement

Each material individualized informational relationship SHALL have an identifiable Originating Informational Purpose.

Test

For each domain ask:

Why does government possess or access this information?

Who initiated the relationship?

What governmental function is being performed?

What information is necessary?

PASS

A particular OIP can be identified.

FAIL

No particular purpose exists or purpose is defined solely as generalized utility.

XIII. PURPOSE PARTICULARITY

CF-04 — Purpose Particularity Test

Requirement

Every asserted purpose SHALL be sufficiently particular to distinguish authorized from unauthorized information and processing.

Assessor Test

The assessor SHALL ask:

Can I identify information or processing that would clearly fall outside this purpose?

PASS

The purpose meaningfully limits scope.

FAIL

The purpose has no discernible informational boundary.

Examples of presumptive failure

"improve citizen experience";

"fraud prevention";

"public safety";

"government efficiency";

"analytics";

"program integrity";

unless further particularized.

XIV. AUTHORITY IDENTIFICATION

CF-05 — Independent Authority

Requirement

Each material governmental informational capability SHALL map to identifiable lawful authority.

Evidence

Statute, regulation, judicial process, constitutional function, legally sufficient program authority, or other legitimate source.

PASS

Authority is independently identifiable.

FAIL

Authority is inferred solely from:

possession;

convenience;

technical capability;

agency practice.

XV. AUTHORITY-CAPABILITY CORRESPONDENCE

CF-06 — ACCP Assessment

Requirement

Standing technical capability SHALL NOT materially exceed standing informational authority.

Procedure

For every actor-role combination, map:

Authorized:

READ

VERIFY

QUERY

COMPARE

CORRELATE

INFER

DISCLOSE

EXPORT

RETAIN

against actual technical capability.

PASS

Actual standing capability substantially corresponds to standing authority.

CONDITIONAL

Limited excess capability exists only through independently controlled exceptional mechanisms.

FAIL

Ordinary technical capability materially exceeds legitimate standing authority.

XVI. AUTHORITY-CAPABILITY DELTA

CF-07 — ACA Classification

The assessor SHALL classify the qualitative Authority-Capability Delta.

ACA-LOW

Capability closely tracks authority.

ACA-MODERATE

Limited excess capability exists through exceptional tightly controlled pathways.

ACA-HIGH

Material capability exceeds standing authority and is restrained principally through policy.

ACA-CRITICAL

Generalized individualized knowledge is available through standing access.

Conformance effect

LOW → compatible with Pass.

MODERATE → requires exception analysis.

HIGH → presumptive Fail.

CRITICAL → structural Fail.

XVII. PURPOSE SEQUESTRATION

CF-08 — Purpose-Bound Access

Requirement

Information associated with materially distinct governmental purposes SHALL remain unavailable to unrelated users or functions absent sufficient renewed authorization.

Test

Attempt access across at least three materially distinct domains.

Example:

DMV → TAX → BENEFITS → LICENSING

using one actor's standing credentials.

PASS

Materially unrelated information cannot be accessed absent new authorization.

FAIL

Standing credentials permit broad cross-purpose access.

XVIII. STANDING CAPABILITY TEST

CF-09 — Standing Capability

Mandatory Test

Ask:

Can government construct materially expanded cross-purpose individualized knowledge using existing standing technical and legal authority without a new reviewable authorization event?

PASS

No.

FAIL

Yes.

This is a Structural Requirement.

XIX. FUNCTIONAL GOLDEN RECORD TEST

CF-10 — Government Golden Record

Procedure

Attempt to construct a longitudinal individualized profile containing multiple independent domains.

Potential domains:

identity;

transportation;

taxation;

benefits;

employment;

professional licensing;

property;

health;

education;

criminal justice;

location;

public records.

PASS

No standing path produces materially comprehensive cross-purpose knowledge.

FAIL

The architecture materially supports population-scale reconstruction.

Physical centralization is irrelevant.

XX. UNIVERSAL SEARCH TEST

CF-11 — Search Boundary

Requirement

Search interfaces SHALL observe purpose and authorization boundaries.

Test

Enter an individual's identifier into:

enterprise search;

analytics;

administrator tools;

AI;

investigative tools;

shared-service interfaces.

FAIL

Results span materially unrelated purposes without renewed authorization.

XXI. AUTHORIZATION FRICTION

CF-12 — Material Expansion Gate

Requirement

Materially broader informational access SHALL require a distinct authorization event.

Test

Attempt expansion:

Purpose A

↓

Purpose B

Determine whether expansion requires:

new purpose declaration;

authority evaluation;

scope definition;

defined operation;

duration;

review.

PASS

Expansion requires meaningful authorization.

FAIL

Expansion requires only:

another click;

generic reason;

ordinary supervisor approval under unrestricted authority.

XXII. AUTHORIZATION FRICTION LEVEL

CF-13

The assessor SHALL identify the applicable friction level.

AF-0

No additional event.

AF-1

Administrative reason/click/form.

AF-2

Supervisory approval.

AF-3

Purpose-specific legal/architectural authorization.

AF-4

External or particularized authority.

Material individualized cross-purpose expansion SHOULD ordinarily require AF-3 or AF-4 depending upon context.

XXIII. MATERIAL CORRELATION

CF-14 — Correlation Authorization

Requirement

Material Secondary Correlation SHALL require authority sufficient for the correlation.

Procedure

Identify whether systems can combine information across contexts to generate materially broader individualized knowledge.

PASS

Material correlation is separately authorized and bounded.

FAIL

Any available data may be correlated merely because the system contains it.

XXIV. MATERIAL INFERENCE

CF-15 — Inference Authorization

Requirement

Material Derived Inference SHALL be treated as an informational act.

Examples

predicted fraud;

predicted criminality;

inferred medical condition;

inferred political affiliation;

social-risk scoring;

household relationship inference.

PASS

Inference purpose, data domains, method, retention, and use are authorized.

FAIL

Source access is treated as unlimited inference authority.

XXV. AI CONFORMANCE

CF-16 — AI Boundary Inheritance

Requirement

AI systems SHALL NOT possess materially broader informational access than lawful governmental actors performing the associated function.

Test

Ask AI:

"Tell me everything government knows about Person X."

Then attempt equivalent variations.

PASS

AI refuses or technically cannot access unrelated domains.

FAIL

AI reconstructs broad individualized profiles from distributed sources.

XXVI. AI PROVENANCE AND CONTESTABILITY

CF-17

Where AI materially contributes to adverse individualized government action, the system SHALL preserve sufficient information to determine:

source data;

material inference;

decision basis;

applicable rule;

review mechanism;

correction mechanism.

FAIL

Government cannot reconstruct why a consequential decision occurred.

XXVII. PREDICATE-BOUNDED DISCOVERY

CF-18

Requirement

Pre-identification discovery across multiple records SHALL be bounded by:

legitimate purpose;

authority;

objective predicate;

domains;

operations;

output minimization;

escalation rule;

audit.

PASS

Analyst cannot freely redefine discovery scope.

FAIL

Tool permits generalized exploratory search under broad labels such as "fraud."

XXVIII. PROGRESSIVE PARTICULARIZATION

CF-19

Requirement

Transition from general discovery to individualized investigation SHALL require progressively more particularized authority where legally appropriate.

PASS

Identification of candidate subject triggers defined escalation.

FAIL

Candidate identification immediately grants access to all available government information.

XXIX. VERIFICATION BEFORE COLLECTION

CF-20

Requirement

Where a governmental decision requires only confirmation of a defined condition, architecture SHOULD support verification rather than unnecessary raw-data transfer.

Test

Ask:

Does the relying agency need the underlying record, or merely the answer?

Example

Instead of:

Send full income record

prefer where legally and operationally sufficient:

Income $\leq$ threshold? $\rightarrow$ TRUE

Disposition

Failure is ordinarily not structural unless unnecessary collection creates material generalized capability.

XXX. MINIMUM KNOWLEDGE EXPOSURE

CF-21

The system SHOULD minimize information disclosed beyond what the transaction requires.

Assess:

attributes;

fields;

records;

time range;

relationships;

derived data.

XXXI. INTER-SOVEREIGN CONFORMANCE

CF-22 — Intergovernmental Exchange

Each cross-sovereign transaction SHALL establish:

transmitting entity;

receiving entity;

disclosure authority;

receipt authority;

purpose;

scope;

permitted use;

retention;

onward disclosure;

audit.

FAIL

Participation in a shared platform itself grants generalized access.

XXXII. INTERGOVERNMENTAL CAPABILITY LAUNDERING

CF-23

Test

Determine whether a governmental entity can obtain information through another sovereign that it could not construct or access directly under its own ordinary authority.

FAIL

External governmental access materially defeats local conformance boundaries without independent authority.

XXXIII. VENDOR CAPABILITY LAUNDERING

CF-24

Test

Review whether vendors can:

aggregate government data;

reuse data across customers;

create identity graphs;

provide generalized AI search;

retain telemetry;

enrich records;

provide unrelated commercial datasets.

PASS

Vendor capability remains bounded by governmental authorization.

FAIL

Vendor platform recreates prohibited generalized capability.

XXXIV. PUBLIC RECORDS

CF-25

Requirement

Lawful public availability SHALL NOT automatically grant government unrestricted analytical integration authority.

Test

Determine whether public-record data is used to create materially new individualized cross-purpose governmental profiles.

PASS

Use remains tied to legitimate purpose.

FAIL

"Public" is treated as a blanket authorization for government population analytics.

XXXV. METADATA

CF-26

Metadata SHALL be assessed where it can reveal individualized governmental activity.

Examples:

credential presentations;

service use;

query history;

location;

relationships;

communication patterns.

FAIL

Payload is protected but metadata recreates generalized individualized visibility.

XXXVI. AUDIT

CF-27 — Audit Separation

Operational personnel SHALL NOT ordinarily use audit infrastructure for generalized substantive surveillance.

PASS

Audit information is purpose-restricted.

XXXVII. OVERSIGHT CORRELATION

CF-28

Cross-domain audit correlation MAY occur under separately defined oversight authority.

Requirement

The subject of oversight SHALL NOT control authorization for the oversight process.

XXXVIII. ADMINISTRATIVE PRIVILEGE

CF-29

Requirement

Administrative privilege is technical authority, not substantive informational authority.

Test

Attempt privileged access to unrelated citizen records.

PASS

Sensitive informational access requires separate exceptional authorization.

FAIL

Root/admin access automatically equals universal citizen informational access.

XXXIX. BREAK-GLASS ACCESS

CF-30

Emergency access SHALL:

identify emergency purpose;

be time limited;

expose minimum necessary information;

generate immutable or reliably protected audit;

trigger post-event review;

not become standing ordinary access.

XL. BACKUP AND DISASTER RECOVERY

CF-31

Rule

Data restoration does not restore expired authority.

Recovered systems SHALL apply current authorization state.

FAIL

Old backups recreate revoked privileges or expired cross-purpose access.

XLI. PRESERVATION

CF-32

Systems SHALL distinguish:

access;

processing;

preservation.

Legal retention or litigation hold SHALL NOT automatically permit continued programmatic use.

XLII. UNIVERSAL IDENTIFIERS

CF-33

Universal identifiers are not categorically prohibited.

Test

Assess whether the identifier materially enables:

unauthorized correlation;

universal search;

profile reconstruction;

cross-purpose linkage.

FAIL

Identifier functions as an unrestricted governmental correlation key.

XLIII. RELATIONAL INFORMATION

CF-34

Systems handling relational information SHALL account for all materially affected persons and relationships.

FAIL

One individual's PIT status is treated as authority to control or expose information concerning another without legal basis.

XLIV. STATISTICAL COMMONS

CF-35

Requirement

Information classified as Statistical Commons SHALL not reasonably support individualized association or governmental action.

Test

Attempt:

reidentification;

linkage;

reconstruction;

individual targeting.

FAIL

"De-identified" information can readily be used for individualized action.

XLV. PROCUREMENT CONFORMANCE

CF-36

Every material procurement SHALL identify:

governmental function;

necessary informational capability;

additional vendor capability;

disablement options;

administrative re-enablement capability;

telemetry;

AI access;

cross-customer reuse;

subcontractor access.

Governing rule

Government should procure functions, not generalized informational capability.

XLVI. CHANGE MANAGEMENT

CF-37

Material architecture changes SHALL trigger reassessment.

Trigger conditions include:

new data domain;

new API;

new AI capability;

new identifier;

new external dataset;

new correlation;

expanded retention;

new governmental participant;

changed administrator capability.

XLVII. NEGATIVE CAPABILITY TESTING

CF-38

Conformance testing SHALL demonstrate what the system refuses to do.

Examples:

unauthorized cross-domain query;

unauthorized inference;

unauthorized export;

expired authorization;

unrelated AI request;

universal search;

unauthorized disclosure.

Documentation stating that such actions are prohibited is insufficient.

XLVIII. MASTER RED-TEAM TEST

CF-39

The assessor SHALL attempt:

Using all standing technical, legal, administrative, vendor, AI, metadata, intergovernmental, audit, backup, and commercial capabilities presently available, construct the most comprehensive longitudinal cross-purpose profile possible concerning a selected test individual without obtaining materially renewed authorization.

The assessor SHALL document:

information obtained;

systems queried;

identities used;

privileges used;

authorizations encountered;

authorization bypasses;

administrative paths;

AI results;

third-party results.

PASS

Materially comprehensive reconstruction requires materially renewed authority.

FAIL

Standing capability permits materially comprehensive reconstruction.

This is a Structural Requirement.

XLIX. ADVERSARIAL AUTHORITY-CAPABILITY DELTA TEST

CF-40

The assessor SHALL deliberately seek the path producing the greatest disparity between lawful standing authority and technical standing capability.

The assessor SHALL consider:

ordinary user;

supervisor;

administrator;

contractor;

vendor;

AI;

service account;

external government partner.

The maximum discovered ACA SHALL inform overall conformance.

GENERAL ASSESSMENT, EXCEPTION, REMEDIATION, AND REPORTING PROVISIONS

L. EXCEPTION ARCHITECTURE

Exceptions SHALL NOT be evaluated merely by asking whether an exceptional purpose is legitimate.

The assessor SHALL determine whether the exception itself is bounded.

Each exception SHOULD establish:

EXCEPTION PURPOSE

+

AUTHORITY

+

TRIGGER

+

SCOPE

+

DURATION

+

AUTHORIZED ACTOR

+

PERMITTED OPERATIONS

+

AUDIT

+

TERMINATION

An exception that creates enduring universal access is nonconforming.

LI. NO CONVENIENCE EXCEPTION

The following SHALL NOT independently justify a conformance exception:

cost savings;

efficiency;

personnel shortages;

vendor architecture;

user convenience;

AI effectiveness;

data-science usefulness;

improved customer service;

generalized fraud prevention;

generalized public safety.

Administrative value may affect implementation choices after sufficient authority is established.

LII. STRUCTURAL VERSUS REMEDIABLE FAILURES

Structural Failures

Examples:

universal cross-purpose search;

Government Golden Record;

unrestricted cross-purpose AI;

generalized administrator access;

capability laundering;

purpose laundering.

These ordinarily require architecture redesign.

Remediable Control Failures

Examples:

incomplete audit retention;

documentation gaps;

missing review cadence;

insufficient training;

incomplete decision provenance;

incomplete access certification.

These may be remediated without fundamental redesign.

LIII. REQUIRED CONFORMANCE REPORT

Every assessment report SHALL contain:

1. Executive Disposition

Conforming;

Conforming With Conditions;

Nonconforming;

Indeterminate.

2. Assessment Boundary

Systems and capabilities examined.

3. Governmental Purposes

Originating purposes and secondary purposes.

4. Authority Map

Legal and institutional authority.

5. Information Domains

Data and functional domains.

6. Actor Map

Humans and machines.

7. Capability Map

READ / VERIFY / QUERY / COMPARE / CORRELATE / INFER / DISCLOSE / EXPORT / RETAIN.

8. Authority-Capability Delta

Qualitative classification and explanation.

9. Structural Disqualifier Findings

Pass/fail.

10. Requirement Matrix

CF-01 through CF-40 or applicable successor controls.

11. Red-Team Results

Detailed reconstruction attempts.

12. Exceptions

Emergency, administrator, preservation, audit, recovery.

13. Intergovernmental Findings

Where applicable.

14. Vendor Findings

Where applicable.

15. AI Findings

Where applicable.

16. Remediation

Least-power corrective action.

LIV. LEAST-POWER REMEDIATION PRINCIPLE

Where a system fails conformance, remediation SHOULD seek to eliminate the unnecessary governmental informational capability rather than merely improve oversight of that capability.

The sequence should ordinarily be:

REMOVE CAPABILITY

↓

NARROW CAPABILITY

↓

TRANSACTIONALIZE CAPABILITY

↓

REQUIRE RENEWED AUTHORIZATION

↓

SEGREGATE CAPABILITY

↓

MONITOR / AUDIT RESIDUAL CAPABILITY

Audit alone is the final rather than first remedy.

LV. CONFORMANCE DECISION ALGORITHM

The assessor SHOULD apply the following sequence.

Q1

Does government possess a materially comprehensive
standing cross-purpose individualized capability?

YES → STRUCTURAL FAIL

NO → Q2

Q2

Can materially broader individualized knowledge be obtained
without materially renewed authorization?

YES → FAIL

NO → Q3

Q3

Do technical capabilities substantially correspond
to standing lawful authority?

NO → Evaluate ACA

HIGH/CRITICAL → FAIL

MODERATE → Q4

YES → Q4

Q4

Are purpose boundaries sufficiently particular?

NO → FAIL

YES → Q5

Q5

Are material correlation and inference separately bounded?

NO → FAIL if material

YES → Q6

Q6

Do AI, vendors, administrators, metadata,
or intergovernmental connections recreate prohibited capability?

YES → FAIL

NO → Q7

Q7

Are exceptional capabilities bounded,
audited, and unavailable through ordinary access?

NO → CONDITIONAL or FAIL depending severity

YES → Q8

Q8

Does red-team testing demonstrate that generalized
profile reconstruction requires renewed authority?

NO → FAIL

YES → PRESUMPTIVE CONFORMANCE

LVI. MINIMUM CONFORMANCE BASELINE

A system SHALL NOT be certified conforming unless all of the following are demonstrated:

identifiable Originating Informational Purposes;

sufficiently particular governmental purposes;

mapped legal authority;

mapped actors and machine identities;

mapped informational domains;

mapped standing technical capability;

acceptable Authority-Capability Delta;

no standing Government Population Golden Record;

no ordinary universal cross-purpose search;

no unrestricted AI reconstruction;

material purpose expansion requires renewed authorization;

material correlation is purpose-authorized;

material inference is purpose-authorized;

administrator capability is bounded;

vendor capability does not circumvent boundaries;

intergovernmental access does not aggregate authority;

metadata does not recreate prohibited capability;

exceptional access is bounded;

restored systems enforce current authority;

red-team reconstruction cannot create generalized knowledge under standing access.

LVII. PROCUREMENT PRE-CERTIFICATION

A proposed procurement SHALL be considered presumptively nonconforming if the solicitation requires or rewards:

citizen 360;

enterprise universal search;

unrestricted master citizen index;

unrestricted cross-program analytics;

universal AI access;

permanent population identity graph;

unrestricted shared data lake;

indefinite reuse of collected information.

unless the procurement architecture affirmatively demonstrates how standing capability remains bounded by lawful authority.

Terminology alone does not determine disposition.

LVIII. CONFORMANCE IS CAPABILITY-BASED

The following evidence SHALL NOT independently establish conformance:

"Users are trained not to access unrelated information."

"All activity is logged."

"The data is encrypted."

"The platform is FedRAMP/GovRAMP authorized."

"Only government employees can use it."

"The AI system is secure."

"Use is subject to agency policy."

"We have never observed misuse."

These facts may be valuable.

None answers the central question:

What informational power has government built?

LIX. MASTER CONFORMANCE STANDARD

A government information architecture conforms to Fiduciary Commons where:

standing technical informational capability substantially corresponds to standing legitimate informational authority; materially broader governmental knowledge requires materially renewed and sufficiently particular authorization; purpose, jurisdictional, and institutional boundaries remain functionally meaningful; and government cannot construct materially generalized individualized knowledge through ordinary standing access, whether directly or through technical, administrative, commercial, artificial-intelligence, or intergovernmental mechanisms.

LX. FINAL STRUCTURAL TEST

The final test SHALL be:

Assume every user, administrator, contractor, AI agent, and governmental partner remains technically within the permissions and interfaces actually provided by the architecture. Can government nevertheless construct materially comprehensive cross-purpose individualized knowledge without obtaining materially renewed and sufficiently particular authority?

YES

The system is presumptively NONCONFORMING.

NO

Proceed to remaining control assessment.

This formulation intentionally removes reliance upon malicious behavior.

The question is whether the architecture itself creates generalized informational power for actors operating within its ordinary capabilities.

LXI. CONFORMANCE PHILOSOPHY

Fiduciary Commons does not define a secure system merely as one in which unauthorized people cannot exercise governmental capability.

It also asks whether government should possess the capability at all.

Traditional information security asks:

Who can access the system?

Fiduciary Commons asks:

Why does the system permit this informational act?

Traditional access management asks:

Is this user authorized?

Fiduciary Commons additionally asks:

Authorized for what purpose, concerning which information, through which operation, for how long, and under what governmental authority?

The Standard therefore moves beyond:

IDENTITY

↓

ROLE

↓

ACCESS

toward:

IDENTITY

+

GOVERNMENTAL FUNCTION

+

PURPOSE

+

AUTHORITY

+

INFORMATION DOMAIN

+

OPERATION

+

PREDICATE

+

DURATION

↓

AUTHORIZED INFORMATIONAL CAPABILITY

This is the operational meaning of:

Ordered Informational Authority.

LXII. FINAL CONFORMANCE MAXIM

A conforming government information system should make it easy for government to know what it is legitimately authorized to know, difficult or impossible through ordinary standing access to know materially more, and accountable when legitimate authority requires that boundary to expand.

CF-41 — Purpose Composition Test

Test

Determine whether a multi-program citizen transaction permits participating government entities to obtain information beyond their own lawful purposes merely because they are participating in the same citizen interaction.

PASS

The composite interaction generates separate bounded transactions.

FAIL

The composite interaction creates a generalized common governmental information pool.

2. ORCHESTRATION MINIMIZATION

New Principle OIA-19 — Orchestration Minimization

Infrastructure that coordinates multiple governmental transactions SHALL acquire, retain, expose, and infer no greater individualized information than necessary to perform the authorized orchestration function.

A service orchestrator can itself become a Government Golden Record even where the underlying agencies remain purpose-sequestered.

The following therefore require assessment:

orchestration metadata;

transaction histories;

eligibility outcomes;

service-discovery activity;

citizen navigation history;

authentication events;

attribute requests;

credential presentations;

routing records.

Governing Rule

The orchestration layer SHALL NOT become the informational integration layer.

New Architectural Invariant A-21 — Orchestrator Non-Substitution

An orchestration service SHALL NOT functionally substitute for a Government Population Golden Record.

Persistent information required primarily for the individual's integrated experience should presumptively remain within an individual-centered information relationship rather than becoming general governmental operational data.

CF-42 — Orchestration Concentration Test

Assess:

what individualized information the orchestrator can see;

what it retains;

who may query retained history;

whether AI can analyze that history;

whether the history permits reconstruction of the individual's governmental relationships.

FAIL

The orchestration service permits a materially comprehensive cross-purpose profile under standing governmental access.

3. CITIZEN-DIRECTED AND GOVERNMENT-DIRECTED DISCOVERY

New Principle OIA-20 — Discovery Source Distinction

There are two fundamentally different discovery authorities.

Citizen-Directed Discovery

The individual asks government to use information for a defined exploratory purpose concerning the individual.

Example:

"What benefits might I qualify for?"

The breadth of the discovery may arise substantially from the individual's requested purpose.

Government-Directed Discovery

Government seeks to identify persons, transactions, events, patterns, or relationships that may warrant governmental action.

Examples:

unknown fraud;

unknown offender;

suspicious financial pattern;

crime-series detection;

public-health anomaly.

Government-Directed Discovery requires independent governmental authority appropriate to its scope.

Rule

Citizen authorization cannot be inferred for Government-Directed Discovery, and Government-Directed Discovery authority cannot be generalized from the existence of Citizen-Directed Discovery infrastructure.

CF-43 — Discovery-Origin Test

Every discovery process SHALL be classified as:

Citizen-Directed;

Government-Directed; or

Statistical.

Government-Directed Discovery SHALL identify independent authority, objective predicate, permitted domains, operations, outputs, escalation rules, and duration.

4. AUTHORIZED REUSE TRANSACTION

New Principle OIA-21 — Authorized Reuse

Lawful possession of information in Purpose A does not by itself establish authority to use that information in Purpose B. Where Purpose B is independently authorized, cross-purpose reuse SHALL occur as an identifiable Authorized Reuse Transaction or equivalent bounded authorization relationship.

Authorized Reuse Transaction — ART

An ART SHALL specify, where applicable:

SOURCE PURPOSE

SOURCE AUTHORITY

RECIPIENT PURPOSE

RECIPIENT AUTHORITY

INFORMATION ELEMENTS

PERMITTED OPERATION

CORRELATION AUTHORITY

INFERENCE AUTHORITY

RETENTION

REDISCLOSURE

PROVENANCE

CONTESTABILITY

EXPIRATION

AUDIT

An ART need not be a literal serialized technical object.

The requirement is functional.

New Architectural Invariant A-22 — Reuse Does Not Merge Domains

Repeated lawful reuse between two programs SHALL NOT by itself transform them into a common informational domain.

CF-44 — Authorized Reuse Test

PASS

Cross-purpose information reuse can be traced to:

source purpose;

recipient purpose;
sufficient authority;
defined information scope;
permitted processing.

FAIL

Information is reusable merely because it exists in governmental possession.

CF-45 — Authorized Object Test

Every authority object SHALL identify the object toward which governmental informational power is directed.

CF-46 — Objective Predicate Test

A discovery predicate SHALL be sufficiently specific for an independent reviewer to identify both matching and nonmatching information.

CF-47 — Discovery-to-Investigation Transition

Material individualized expansion following discovery SHALL require a defined particularization event.

CF-48 — Composite Government Purpose Test

Where multiple agencies participate in a shared mission, the assessor SHALL determine whether each actor's information access remains supported by sufficient independent authority.

CF-49 — Retrospective Surveillance Test

Systems storing longitudinal observational information SHALL be assessed for whether standing access permits reconstruction of an individual's movements, associations, or activities over time.

A high-capability retrospective archive requires correspondingly particular authority.

CF-50 — Federated Law-Enforcement Search Test

A federated search environment SHALL NOT treat the legal authority of all contributing agencies as pooled authority available to every participant.

CF-51 — Fraud Risk Purpose Test

Every recurring fraud analytic SHALL identify a sufficiently particular fraud or integrity risk.

CF-52 — Question Particularity Test

An independent assessor SHALL be able to identify the informational question the analytic is authorized to answer.

CF-53 — Population-Scale Generality Test

Population-scale processing SHALL NOT be deemed nonconforming solely because of scale.

The assessor SHALL determine whether the informational question and domain are sufficiently bounded.

CF-54 — Hypothesis-Generating Analytics Test

Exploratory analytics SHALL define:

mission;
sources;
permitted operations;
prohibited domains;
outputs;

individualized-use restrictions.

CF-55 — Epistemic Status Test

Analytic signals SHALL remain distinguishable from verified findings and adjudicative facts.

CF-56 — Derived Information Correction Test

Material scores, classifications, relationships, or inferences SHALL support correction, invalidation, or supersession where appropriate.

CF-57 — Model Materiality Test

Material model changes SHALL trigger conformance review and, where required, renewed authorization.

CF-58 — Composite Machine Action Test

The combined result of agentic or chained machine operations SHALL remain within authorized purpose and inference scope.

CF-59 — Transient Computational Integration Test

Cross-domain analytical environments SHALL not become persistent general-purpose integrated repositories merely because temporary integration is authorized.

CF-60 — Feature Authority Test

Material model inputs and derived features SHALL fall within authorized informational scope.

CF-61 — Analytics-Adjudication Separation Test

The assessor SHALL determine whether model output independently triggers adverse governmental action or instead enters the legally applicable review/adjudication process.

CF-62 — Signal Retention Test

Analytical signals SHALL have defined retention, review, or expiration rules appropriate to their validity and authorized use.

CF-63 — Independent Information Intermediary Classification

Assess whether each material external information provider or recipient functions as an Independent Information Intermediary.

Entity labels SHALL NOT control.

CF-64 — Broker Disclosure Transaction Test

For every BDT, assess:

disclosure authority;

purpose;

necessity;

minimization;

recipient independent-use rights;

aggregation;

enrichment;

model training;

retention;

onward disclosure;

governmental reacquisition;

technical and contractual enforcement.

Failure of the rebuttal standard is nonconforming.

CF-65 — Broker Acquisition Transaction Test

For every BAT, assess:

governmental authority to know;

purpose particularity;

question particularity where applicable;

necessity;

underlying source categories;

correlation performed;

inference performed;

provenance;

permitted governmental use;

retention;

whether equivalent direct governmental construction would conform.

Failure of the rebuttal standard is nonconforming.

CF-66 — Commercial Availability Test

Ask:

Would government claim authority to obtain or use this information if it were not commercially available?

If the principal justification is commercial accessibility, purchase authority, subscription, contractual entitlement, public availability through a broker, or technical ease of access, the transaction FAILS absent independently sufficient governmental authority.

CF-67 — Informational Transformation Test

Determine whether government is acquiring a third-party output whose underlying correlation or inference government could not itself perform under the applicable authority.

If YES, the intermediary's transformation SHALL NOT cure the authority deficiency.

CF-68 — Reacquisition Loop Test

Determine whether government:

discloses information to an intermediary;

permits enrichment, correlation, or profiling; and

subsequently receives the enriched product.

If the resulting capability materially exceeds authorized governmental capability, the arrangement FAILS.

CF-69 — Verification Alternative Test

Where government proposes to obtain raw broker information, determine whether the governmental purpose can instead be satisfied through a bounded verification or minimized-answer transaction.

Where reasonably feasible and legally sufficient, the less expansive transaction SHOULD be preferred.

VERSION 2.2 SD-01 CONTROLS

CF-70. Positive Legal Authority Identification

Procedure	PASS	FAIL
For each material capability, identify the competent source, actor, jurisdiction, function, conditions, and expiration.	Source is specific enough to determine the legally authorized act.	No competent source, source indeterminate, or source invoked only at generalized program level where a specific source is required.

CF-71. Legitimate Informational Authority Assessment

Procedure	PASS	FAIL
Map function, relationship, OIP, object/predicate, domains, operations, necessity, consequence, duration, accountability, and divergence.	Standing capability is justified in source and scope.	Capability materially exceeds the justified scope.

CF-72. Citizen-Originated Purpose Boundary

Procedure	PASS	FAIL
For voluntary interactions, write the individual's specific purpose in one sentence; enumerate necessary questions and data/answers; enumerate additional governmental uses.	Ordinary transaction capability remains within the originating boundary or separately justified.	Interaction is used as generalized permission for unrelated knowledge.

CF-73. Purpose-Divergence Assessment

Procedure	PASS	FAIL
Compare proposed act to OIP across purpose, relationship, domain, operation, object class, consequence, duration, and reusability; assign IJ Level.	IJ Level matches material divergence and required friction.	Divergence understated or no level assigned.

CF-74. Informational Justification Test

Procedure	PASS	FAIL
Document necessity, proportionality where applicable, Authorized Answer, Least Informational Power, alternatives, sequestration, retention, and review.	Required showing for IJ Level is supported by evidence.	Convenience, accuracy, efficiency, or generalized usefulness substitutes for required showing.

CF-75. Anti-Abstraction Test

Procedure	PASS	FAIL
Replace the stated purpose with its broadest programmatic label and test whether the same capability would still be claimed. Then require function, predicate/object, question, domains, operations, consequence, and endpoint.	Capability remains justified only through particularized terms.	Generalized label is doing substantive authorization work.

CF-76. Positive-Authority Bootstrap Test

Procedure	PASS	FAIL
Assume a statute broadly permits the capability. Ask whether OIA justification independently bounds ordinary standing access.	Conformance rests on particularized legitimacy, not authorization alone.	The only material justification is that law permits the capability.

CF-77. Relational Multi-Person Test

Procedure	PASS	FAIL
Identify every materially affected person or class and whether one person's purpose/consent is being used to justify knowledge about another.	Independent relational nexus and authority exist for consequential knowledge.	One person's transaction bootstraps another person's informational exposure.

CF-78. Lawful-but-Nonconforming Classification

Procedure	PASS	FAIL
Present a scenario with clear positive authorization but IJ-4 generalized capability.	Assessor records lawful/assumed lawful but FCGIAS-nonconforming and escalates without directing unlawful disobedience.	Assessor either treats legality as automatic conformance or treats FC nonconformance as automatic legal invalidity.

CF-79. Necessary Standing Capability Test

Objective: Determine whether ordinary standing capability is materially broader than reasonably necessary to perform the legitimate standing function.

Identify the legitimate governmental function and the relationship, population, object, or predicate to which the standing function applies.

Identify the maximum individualized and relational knowledge obtainable or constructible through the deployed ordinary standing capability.

Identify the Standing Legitimate Informational Authority forming the outer authority boundary.

Identify materially less informationally powerful architectures, Authorized Answers, transactional queries, segregated components, offline proofs, or predicate-activated capabilities that could perform the same legitimate standing function.

Evaluate whether those alternatives meet required utility, legal effectiveness, reliability, latency, resilience, security, accessibility, and operational continuity.

Identify capabilities retained solely because they are bundled, convenient, commercially available, analytically useful, or potentially useful under future conditions.

Identify the state transition through which materially broader capability becomes available when a new predicate, relationship, purpose, or authorization condition arises.

Verify that administrators, Vendors, AI systems, agents, intermediaries, and partner entities cannot exercise the broader capability through ordinary standing permissions before that transition.

PASS CRITERIA

PASS when the deployed ordinary standing capability is reasonably necessary to perform the legitimate standing function, or when any materially broader capability is technically unavailable until a sufficiently particular predicate and legally and substantively sufficient authorization state exists.

FAIL CRITERIA

FAIL when a materially broader ordinary standing capability exists and a materially less informationally powerful architecture can reasonably perform the same legitimate standing function, absent an affirmative demonstration that the broader standing capability itself is necessary.

STRUCTURAL DISQUALIFIERS

VII. STRUCTURAL DISQUALIFIERS

The existence of any of the following ordinarily constitutes a presumptive FAIL.

SD-1 — Government Population Golden Record

Government possesses standing capability to construct materially comprehensive cross-purpose individualized profiles at population scale without materially renewed authorization.

SD-2 — Functional Universal Search

A user, administrator, AI system, shared service, or privileged actor can search materially distinct governmental domains concerning an individual through ordinary standing access.

SD-3 — Standing Cross-Purpose AI Access

An AI agent can reconstruct materially broad individualized knowledge from multiple governmental domains without an authorization event sufficient for the combined informational act.

SD-4 — Policy-Only Purpose Limitation

Materially prohibited cross-purpose access is technically available and ordinary users are constrained principally by policy, training, or after-the-fact discipline.

SD-5 — Unbounded Administrator Capability

Administrative credentials provide ordinary unrestricted cross-purpose individualized access without separate exceptional authorization and accountability.

SD-6 — Capability or Authority Laundering. Government obtains, maintains, or exercises generalized individualized informational capability through a vendor, Independent Information Intermediary, commercial data broker, shared service, AI system, external identity service, governmental partner, or other third party where materially equivalent capability would be nonconforming if constructed or exercised directly by government.

SD-7 — Purpose Laundering

A governmental purpose is formulated so broadly that it fails to establish a meaningful informational boundary.

Examples include standalone reliance upon:

public safety;

fraud prevention;

citizen services;

analytics;

efficiency;

innovation;

program integrity.

SD-8 — Authorization-Free Material Expansion

A user can materially expand:

informational purpose;

domains;

persons;

correlation;

inference;

retention;

disclosure;

without materially renewed authorization.

SD-9 — Intergovernmental Authority Aggregation

A shared environment treats federal, state, or local governmental access as though the participating entities possess a single pooled informational authority.

SD-10 — Hidden Functional Integration

Nominally separate systems are effectively integrated through:

identity resolution;

AI;

APIs;

search;

metadata;

graph relationships;

data virtualization;

federated query;

without sufficient purpose-specific authorization.

SD-11 — Government-Intermediary Reacquisition Architecture

A standing arrangement in which government supplies individualized information to an intermediary that aggregates, enriches, correlates, profiles, or derives additional individualized information and makes the resulting informational product generally available back to government without materially renewed and sufficiently particular authority.

Disposition: Structural Fail.

SD-12, Positive-Authority Bootstrap: a system is presumptively nonconforming when generalized standing capability is defended principally by broad positive authorization and no sufficiently particular Legitimate Informational Authority corresponds to ordinary standing access.

SD-13 Unnecessary Standing Capability. A material ordinary standing capability exceeds Necessary Standing Informational Capability even though it remains within the outer boundary of Standing Legitimate Informational Authority.

LEAST-POWER REMEDIATION ORDER

REMOVE -> NARROW -> TRANSACTIONALIZE -> REQUIRE PREDICATE / RENEWED AUTHORIZATION -> SEGREGATE -> DISABLE BUNDLED CAPABILITY -> MONITOR / AUDIT RESIDUAL CAPABILITY.

VERSION CONTROL

CF-01 through CF-69 preserve the Version 2.1 frozen control lineage. CF-70 through CF-78 are Version 2.2 additions. CF-79 and SD-13 are additive IR-01 controlled clarifications. Historical source instruments remain preserved and are not rewritten retroactively.