FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD

Version 2.2 Candidate Standard

Consolidated Controlling Edition, including IR-01 controlled clarification

12 September 2026

CONTROLLED STATUS AND READING RULE

This consolidated edition assembles in one document the complete Version 2.1 historical baseline together with every controlling Version 2.2 substantive delta, the Version 2.2 Candidate Standard designation, the adopted IR-01 clarification, and the T-70 / CF-79 / SD-13 controlled extension. It introduces no new substantive rule.

The Version 2.2 and IR-01 provisions reproduced in Parts A through D control wherever they revise, clarify, or supplement the inherited Version 2.1 baseline reproduced in Part E. Version 2.1 provisions not expressly revised remain operative without substantive change. This compilation preserves original section numbering and provenance rather than silently renumbering or rewriting inherited provisions.

Accordingly, this document is a complete controlling compilation for readers. It should be cited as FCGIAS Version 2.2 Candidate Standard, Consolidated Controlling Edition (Sept. 12, 2026).

ACRONYM

FCGIAS means Fiduciary Commons Government Information Architecture Standard.

PART A. VERSION 2.2 CANDIDATE STANDARD DESIGNATION AND FREEZE RECORD

FCGIAS VERSION 2.2

Candidate Standard Designation and Freeze Record

Ordered Informational Authority with Legitimate Informational Authority | 10 September 2026

DESIGNATION

Following controlled integration of FC-P2.1-SD-01 and a second whole-system adversarial audit resulting in PASS with no Priority 1 or Priority 2 defect requiring reopening, FCGIAS Version 2.2 is designated the Candidate Standard for the Fiduciary Commons Government Information Architecture Standard development record.

SUBSTANTIVE CHANGE FROM VERSION 2.1

Version 2.2 makes explicit that governmental informational power is not conforming merely because a competent legal source authorizes it. Positive Legal Authority and Legitimate Informational Authority are distinct. ACCP now compares standing technical capability with Standing Legitimate Informational Authority. Materially Renewed Authorization must be both legally sufficient and substantively sufficient under Ordered Informational Authority.

CONTROLLING PROGRESSION

Delegated Public Authority → Legitimate Governmental Function → Originating Informational Purpose → Informational Justification → Legitimate Informational Authority → OIA → ACCP → FCGIAS

CITIZEN-ORIGINATED PROGRESSION

Individual's Specific Purpose → Necessary Governmental Question → Authorized Answer → Least Informational Power → Legitimate Informational Authority → Corresponding Technical Capability

FREEZE RULE

Version 2.2 Candidate Standard is presumptively substantively frozen. Reopening requires a demonstrated material legal defect, material architectural contradiction, unaddressed real-world use case that cannot reasonably conform, implementation impossibility, or conformance ambiguity likely to produce materially inconsistent assessment outcomes.

STATUS OF VERSION 2.1

Version 2.1 remains preserved as the prior Candidate Standard and historical baseline. It is not rewritten retroactively. FC-P2.1-SD-01 records why Version 2.2 became necessary.

CONTROLLED IMPLEMENTATION WORK REMAINING

- Consolidated 69-row NTM.
- Consolidated CF-01 through CF-78 test suite.
- Clean synchronized PDTA, VIDA, and GAAFA Version 2.2 legislative candidates.
- Updated procurement specification and architecture figure.

- New substantive white-paper edition explaining Version 2.2.

PART B. VERSION 2.2 SUBSTANTIVE INTEGRATION LAYER

FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD

Version 2.2-RC1, Integrated Standard

Release Candidate 1, post-Version 2.1 substantive integration | 10 September 2026

CONTROLLED STATUS

Version 2.2-RC1 incorporates FC-P2.1-SD-01 into the frozen Version 2.1 architecture. Version 2.1 remains the historical prior Candidate Standard. This RC1 does not yet carry Candidate Standard status. Candidate designation is conditioned on the second whole-system audit.

All Version 2.1 provisions not expressly revised below remain in force in RC1 without substantive change. This integration instrument states the complete controlling delta and the resulting normative hierarchy, so that no SD-01 amendment remains an unattached addendum.

PART I. REVISED GOVERNING ARCHITECTURE

§1. Governing Objective, revised

Ordered Informational Authority is the allocation and constraint of governmental informational power according to legitimate relationships, functions, purposes, jurisdiction, and authority. Positive Legal Authority is necessary where applicable but is not self-validating for FCGIAS conformance. Materially broader informational power requires materially renewed authorization that is both legally sufficient and substantively sufficient under Ordered Informational Authority.

§2. Central Architectural Principle, revised

Government SHALL NOT construct, acquire, procure, configure, or maintain standing informational capability materially broader than necessary to exercise Standing Legitimate Informational Authority. Government should possess the informational power necessary to govern lawfully and faithfully, but SHALL NOT transform many limited grants of authority into a standing generalized power to know.

PART II. DOCTRINAL STATUS

§3. D3 Classification of SD-01

The Positive Legal Authority / Legitimate Informational Authority distinction, Purpose-Divergence Principle, Informational Justification Levels, and Non-Self-Validation rule are D3 Fiduciary and Architectural Synthesis unless independently made legally binding by constitutional, statutory, regulatory, judicial, or other controlling law. The analogy to heightened constitutional scrutiny is explanatory and SHALL NOT be represented as existing general constitutional doctrine.

PART III. DEFINITIONS

Term	Controlling definition

Positive Legal Authority	Authority supplied by a constitution, statute, regulation within delegated authority, judicial process, lawful administrative authority, individual authorization where legally cognizable, emergency authority, or another competent legal source.
Legitimate Informational Authority	Governmental authority to obtain, verify, know, correlate, infer, disclose, retain, or act upon information that is justified in source and scope by the governmental relationship, function, jurisdiction, Originating Informational Purpose, Authorized Object or predicate, information domains, authorized operations, necessity, proportionality where applicable, duration, permitted consequence, accountability, and Purpose Divergence.
Standing Legitimate Informational Authority	Legitimate Informational Authority exercisable through ordinary standing governmental access without a new authorization transition.
Purpose Divergence	A material departure from the Originating Informational Purpose in purpose, question, domain, operation, object class, consequence, duration, relationship, or reusable standing capability.
Informational Justification Level	The level of justification required under FCGIAS according to Purpose Divergence, materiality, necessity, informational scope, consequence, duration, and standing capability.

PART IV. FOUNDATIONAL PRINCIPLES

F-1A. Non-Self-Validation

Governmental informational authority SHALL be evaluated for legitimacy in both source and scope. Positive authorization does not by itself establish FCGIAS conformance.

F-1B. No Conformance Bootstrap

No statute, regulation, administrative authorization, contract, policy, technical permission, procurement instrument, or platform capability establishes conformance merely because it permits the capability being evaluated.

F-1C. Conformance Non-Usurpation

FCGIAS nonconformance does not, standing alone, render positively authorized conduct unlawful or authorize an official, assessor, Vendor, or system to disregard controlling law. The consequence is classification, disclosure, escalation, lawful remediation, procurement action within authority, or recommendation for legal reform unless governing law independently gives the FCGIAS rule legal effect.

F-1D. Express Democratic Departure

A legislature may expressly enact a rule that departs from FCGIAS as a matter of positive law. Such enactment does not alter the Standard's normative conformance classification unless the Standard itself is amended through controlled versioning. This preserves democratic lawmaking authority while preventing positive authorization from becoming self-validating inside the architecture.

PART V. ORIGINATING INFORMATIONAL PURPOSE AND PURPOSE DIVERGENCE

§4. Citizen-Originated Purpose, revised

Where an individual voluntarily initiates a governmental interaction to obtain a nonmandatory license, permit, benefit, credential, service, status, or other governmental action, the individual's specific purpose presumptively establishes the originating boundary of Legitimate Informational Authority. The interaction is not generalized consent to materially unrelated inquiry, correlation, inference, retention, disclosure, or reuse.

§5. Authority-Originated Purpose, preserved and clarified

Taxation, regulation, investigation, adjudication, enforcement, child protection, public health, emergency response, national security, and other independently authorized governmental functions do not depend on individual consent. Each must nevertheless establish its own Legitimate Informational Authority.

§6. Purpose-Divergence Principle

The required justification SHALL increase as governmental informational power becomes materially more remote from the Originating Informational Purpose, crosses purposes or relationships, increases comprehensiveness or consequence, creates new individualized or relational knowledge, or creates durable or reusable standing capability.

§7. Anti-Abstraction

Government SHALL NOT cure Purpose Divergence by redescribing a purpose at a higher level of abstraction. Efficiency, public welfare, public safety, citizen services, program integrity, fraud prevention, modernization, research, analytics, innovation, security, data-driven government, and administrative convenience are insufficient standing alone.

PART VI. INFORMATIONAL JUSTIFICATION LEVELS

Level	Class	Condition	Minimum showing
IJ-1	Purpose-Constitutive	Intrinsic to resolving the citizen-originated request or performing a sufficiently particular authority-originated function.	Relevance; necessity; Authorized Answer; Least Informational Power; bounded operations; endpoint.
IJ-2	Purpose-Protective	Ancillary but demonstrably necessary to authenticate, secure, or protect the integrity of the same transaction or function.	Substantial nexus; necessity; proportionality; less-informational-power alternatives; sequestration; retention; accountability.
IJ-3	Purpose-Divergent	Materially different objective, relationship, domain, operation, consequence, or reusable capability.	Independent particularized Positive Legal Authority; strong justification for divergence; necessity; proportionality; Least Informational Power; structural segregation; expiration/review; authorization friction.
IJ-4	Purpose-Generalized	Cross-purpose or population-scale reusable capability justified principally by generalized governmental usefulness.	Presumptively nonconforming. Generalized utility alone is insufficient; function, predicate/object, question, domains, operations, consequence, duration, and authorization transition

			must be particularized.

PART VII. MATERIAL EXPANSION AND AUTHORIZATION

§8. Materially Renewed Authorization, revised

Materially Renewed Authorization means a distinct and reviewable authorization event that is both legally sufficient under the applicable legal regime and substantively sufficient under Ordered Informational Authority for the proposed Material Expansion. It SHALL identify, as applicable, Positive Legal Authority, governmental function, relationship or predicate, Originating Informational Purpose, Authorized Object, question, domains, operations, necessity, Purpose Divergence, Informational Justification Level, duration, consequence, accountability, and the structural boundary of expanded capability.

§9. Authorization Friction, revised

Authorization Friction SHALL correspond to the materiality and Purpose Divergence of the expansion. Heightened justification does not necessarily require temporal delay. Predetermined legal and technical conditions may permit rapid or automated transition when all required conditions are satisfied and auditable.

PART VIII. ACCP

§10. ACCP, revised

A conforming governmental information architecture SHALL cause Standing Technical Informational Capability substantially to correspond to Standing Legitimate Informational Authority, not merely to the maximum capability permitted by Positive Legal Authority.

STANDING LEGITIMATE INFORMATIONAL AUTHORITY ≈ STANDING TECHNICAL INFORMATIONAL CAPABILITY

§11. Authority-Capability Delta, revised

ACΔ SHALL be measured against Standing Legitimate Informational Authority. Broad positive legislation, regulation, contract, subscription, platform permission, or commercial availability does not by itself reduce the delta.

§12. Standing Capability Test, revised

Can government construct materially broad cross-purpose individualized or relational knowledge through ordinary standing capability without encountering an authorization transition that is both legally sufficient and substantively sufficient under OIA? If YES, the capability is presumptively nonconforming.

PART IX. CROSS-CUTTING APPLICATION

§13. Authorized Answer and Least Informational Power

Where a governmental function can be performed through a bounded answer, proof, or derived attribute rather than acquisition of the underlying informational environment, the more informationally powerful alternative requires independent justification.

§14. Relational Information

No one person's citizen-originated purpose or consent alone establishes Legitimate Informational Authority for materially consequential knowledge concerning another person. Multi-person effects, relational nexus, independent authority, necessity, and consequence SHALL be assessed.

§15. Artificial Intelligence and Learned Artifacts

AI, automated systems, model features, embeddings, scores, predictions, learned artifacts, and Material Derived Inferences inherit the Legitimate Informational Authority of the governmental function served. Predictive utility and technical availability do not create legitimacy.

§16. Intergovernmental Non-Aggregation

Positive Legal Authority held by one sovereign, agency, program, or actor does not establish Legitimate Informational Authority for another. Each recipient SHALL possess sufficient authority and justification for its own act and consequence.

§17. Vendor Non-Expansion

A Vendor does not become a governmental fiduciary merely by supplying capability. Vendor capability exercisable by government through ordinary arrangements is included in conformance assessment, but Vendor possession, contract, commercial access, or platform functionality does not enlarge governmental Legitimate Informational Authority.

§18. Cybersecurity and Abuse Detection

Cybersecurity may constitute an Authority-Originated Purpose and may justify rapid IJ-2 or IJ-3 activity where sufficiently particular. Security SHALL NOT function as an abstract standing justification for unrelated individualized knowledge.

PART X. PROCUREMENT AND CONFORMANCE

§19. Procurement ACCP, revised

Government SHALL NOT procure, subscribe to, configure, or retain materially broader standing informational capability than Legitimate Informational Authority requires merely because broader capability is bundled, commercially available, convenient, efficient, or positively authorized at a generalized level. Government should procure functions, not generalized informational power.

§20. Conformance-Legality Classification

Assessments SHALL distinguish: (1) lawful and FCGIAS-conforming; (2) lawful but FCGIAS-nonconforming; (3) legal authority disputed or indeterminate; and (4) independently unlawful under applicable law. Conformance and positive-law validity SHALL NOT be collapsed.

§21. Structural Disqualifier SD-12, Positive-Authority Bootstrap

Standing generalized informational capability is presumptively nonconforming where its principal justification is that a broad legal or administrative instrument permits the capability but the architecture cannot identify sufficiently particular Legitimate Informational Authority corresponding to ordinary standing access.

PART XI. NEW CONFORMANCE CONTROLS

Control	Name	Requirement
CF-70	Positive Legal Authority Identification	Identify the competent legal source for each material capability.
CF-71	Legitimate Informational Authority Assessment	Evaluate source and scope under OIA independently of mere positive authorization.
CF-72	Citizen-Originated Purpose Boundary	Identify the individual's specific purpose and information or operations materially outside it.

CF-73	Purpose-Divergence Assessment	Classify divergence and assign IJ Level.
CF-74	Informational Justification Test	Document necessity, proportionality where applicable, Authorized Answer, Least Informational Power, consequence, duration, and alternatives.
CF-75	Anti-Abstraction Test	Verify that conformance does not depend on generalized labels.
CF-76	Positive-Authority Bootstrap Test	Test whether broad authorization is functioning as the sole or principal justification for generalized capability.
CF-77	Relational Multi-Person Test	Test whether one person's purpose or consent is being used to justify consequential knowledge about another.
CF-78	Lawful-but-Nonconforming Classification	Verify that assessment can report FC nonconformance without purporting to invalidate controlling law.

PART XII. REVISED NORMATIVE DEPENDENCY CHAIN

LIMITED DELEGATED GOVERNMENTAL AUTHORITY
↓
POSITIVE LEGAL AUTHORITY IDENTIFIED
↓
LEGITIMATE GOVERNMENTAL FUNCTION + ORIGINATING INFORMATIONAL PURPOSE
↓
INFORMATIONAL JUSTIFICATION / PURPOSE-DIVERGENCE ANALYSIS
↓
LEGITIMATE INFORMATIONAL AUTHORITY
↓
POSSESSION / CAPABILITY / COMMERCIAL AVAILABILITY DO NOT CREATE OR VALIDATE AUTHORITY
↓
MATERIAL EXPANSION REQUIRES LEGALLY AND SUBSTANTIVELY SUFFICIENT RENEWED AUTHORIZATION
↓
ACCP / ACΔ
↓
PURPOSE SEQUESTRATION + AUTHORIZATION FRICTION + LEAST INFORMATIONAL POWER
↓
NO STANDING GENERALIZED INFORMATIONAL POWER

PART XIII. MASTER TESTS

§22. Master Conformance Standard

A conforming architecture causes standing governmental informational capability, including capability exercised through systems, administrators, Vendors, AI, commercial information services, intermediaries, and governmental partners, to substantially correspond to Standing Legitimate Informational Authority. Positive Legal Authority is necessary where applicable but is not self-validating for FCGIAS conformance.

§23. Master Design Question

What is the most extensive individualized or relational knowledge government can obtain or construct through ordinary standing capability, what Legitimate Informational Authority justifies that capability, and what additional legally and substantively sufficient authorization must government obtain before it can know materially more?

§24. Master Fiduciary Question

Is government exercising informational power faithfully to the relationship, function, purpose, and authority that justify that power, or exploiting positive authorization, possession, interoperability, commercial availability, or technical capability to acquire, create, disclose, or use materially broader knowledge?

PART XIV. VERSION CONTROL

Version 2.2-RC1 supersedes Version 2.1 only for purposes of candidate integration testing. Version 2.1 remains the last designated Candidate Standard until the whole-system audit of 2.2-RC1 is complete. No substantive rule in this RC1 is final merely because it appears here.

PART C. IR-01 ADOPTION AND FREEZE UPDATE

FCGIAS VERSION 2.2

IR-01 Adoption and Freeze Update

Controlled post-freeze clarification | 11 September 2026

1. DETERMINATION

Following the IR-01 Narrow Verification, which returned PASS with no Priority 1 or Priority 2 contradiction, the Necessary Standing Informational Capability clarification is adopted as a controlled Version 2.2 interpretive clarification.

2. STATUS OF VERSION 2.2

Version 2.2 remains the Candidate Standard. The pre-IR-01 Candidate Standard and its designation record remain preserved as historical artifacts. This clarification does not retroactively alter those records.

3. CONTROLLING CLARIFICATION

Standing Technical Informational Capability SHALL correspond to, and SHALL NOT materially exceed, Necessary Standing Informational Capability. Necessary Standing Informational Capability SHALL remain within Standing Legitimate Informational Authority.

A broader informational capability that may legitimately become available under future predicates, relationships, or authorization states does not thereby become justified ordinary standing capability.

4. STRUCTURAL LEAST-POWER PRESUMPTION

Where a materially less informationally powerful architecture reasonably performs the same legitimate standing function with the required utility, reliability, security, and legal effectiveness, the broader ordinary standing capability is presumptively nonconforming unless government demonstrates that the broader capability itself is reasonably necessary.

5. REVISED ACCP

A conforming governmental information architecture SHALL cause government's Standing Technical Informational Capability to correspond to, and not materially exceed, its Necessary Standing Informational Capability, which in turn SHALL remain within Standing Legitimate Informational Authority. Materially broader capability MAY become available only when the governmental relationship, predicate, purpose, and authority have expanded sufficiently to justify that capability and the broader capability is reasonably necessary to perform the resulting legitimate function.

6. REVISED AUTHORITY-CAPABILITY DELTA

ACDelta includes both capability beyond Standing Legitimate Informational Authority and capability within that outer boundary that materially exceeds Necessary Standing Informational Capability for the ordinary standing function.

7. REVISED MASTER DESIGN QUESTION

What is the most extensive individualized or relational knowledge government can obtain or construct through ordinary standing capability; what Legitimate Informational Authority justifies the outer boundary of that power; what portion of that capability is actually necessary to perform the legitimate standing function; and what legally and substantively sufficient transition must occur before government becomes capable of knowing materially more?

8. NO PHONE HOME CANONICAL EXAMPLE

No Phone Home is designated a canonical example of the Structural Least-Power Presumption. Where verification can occur without an issuer, identity provider, intermediary, or unrelated governmental actor observing the transaction or acquiring materially additional information, the unnecessary observational capability should be made technically unavailable unless an independent legitimate function establishes its necessity.

9. IJ ORDER OF OPERATIONS

Structural Least Power operates before graduated Informational Justification. Government should first determine whether a materially less informationally powerful architecture can reasonably perform the legitimate function. IJ analysis does not convert an avoidable standing capability into a conforming one merely because the governmental objective is important.

10. CONTROL ADDITIONS

Add T-70, Necessary Standing Informational Capability, and CF-79, Necessary Standing Capability Test.

11. NON-USURPATION

This clarification is a FCGIAS conformance rule unless independently made binding through competent law, regulation, contract, procurement requirement, judicial order, or other legal source. It does not authorize disregard of controlling law.

12. FREEZE

With IR-01 adopted, Version 2.2 remains substantively frozen except for future defects meeting the existing reopening criteria. Publication and implementation artifacts may be updated to reflect this controlled clarification, with provenance preserved.

PART D. IR-01 NORMATIVE TRACEABILITY AND CONFORMANCE EXTENSION

FIDUCIARY COMMONS VERSION 2.2

IR-01 NTM and Conformance Controlled Extension

T-70 and CF-79 | 11 September 2026

A. NORMATIVE TRACEABILITY ADDITION

NTM ID	Normative Proposition	Source	Control	Failure Mode	Required Evidence
T-70	Standing technical capability must not materially exceed Necessary Standing Informational Capability, and Necessary Standing Informational Capability must remain within Standing Legitimate Informational Authority.	IR-01 Adoption and Freeze Update §§ 3-9	CF-79	Unnecessary Standing Capability	Function statement; capability inventory; maximum-knowledge analysis; narrower-architecture alternatives; utility/security/reliability requirements; activation predicates; authorization-transition design; remediation record.

B. CF-79 NECESSARY STANDING CAPABILITY TEST

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

1. Identify the legitimate governmental function and the relationship, population, object, or predicate to which the standing function applies.
2. Identify the maximum individualized and relational knowledge obtainable or constructible through the deployed ordinary standing capability.
3. Identify the Standing Legitimate Informational Authority forming the outer authority boundary.
4. 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.
5. Evaluate whether those alternatives meet required utility, legal effectiveness, reliability, latency, resilience, security, accessibility, and operational continuity.
6. Identify capabilities retained solely because they are bundled, convenient, commercially available, analytically useful, or potentially useful under future conditions.
7. Identify the state transition through which materially broader capability becomes available when a new predicate, relationship, purpose, or authorization condition arises.
8. 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.

C. STRUCTURAL FAILURE LABEL

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.

D. REMEDIATION ORDER

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

E. VERSION CONTROL

T-01 through T-69 and CF-01 through CF-78 remain unchanged by this extension. T-70 and CF-79 are additive controlled clarifications. Any future consolidated NTM or assessor suite should preserve the pre-IR-01 record and identify this extension.

PART E. INHERITED VERSION 2.1 NORMATIVE BASELINE

The following is the complete Version 2.1 Candidate Standard. It remains operative except where Parts A through D expressly revise, clarify, or supplement it.

FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD

Version 2.1 — Candidate Standard

Ordered Informational Authority for Government

Status: Candidate Standard
Primary Application: State and local government
Federal Civil Application: Reference and presumptive applicability according to governing law
National Security / Foreign Intelligence: Foundational principles apply; specialized operational profile required
Architecture: Technology-neutral; architecture-specific
Supersedes: Development Versions 1.0–2.1-RC1

PART I — PURPOSE, SCOPE, AND STATUS

§1. Purpose

The Fiduciary Commons Government Information Architecture Standard ("FCGIAS") establishes principles, architectural requirements, controls, and conformance criteria for governmental information systems.

Its central concern is not merely whether government possesses information lawfully or protects that information from unauthorized access.

It asks a prior architectural question:

What informational power has government built for itself?

FCGIAS seeks to ensure that governmental technical capability remains substantially aligned with legitimate governmental informational authority.

---

§2. Governing Objective

The objective of FCGIAS is **Ordered Informational Authority**.

Ordered Informational Authority is the allocation of the power to obtain, verify, know, correlate, infer, disclose, retain, and act upon information among individuals, fiduciaries, institutions, and governments according to legitimate relationships, purposes, jurisdiction, and authority, such that materially broader informational power requires materially renewed authorization and cannot arise merely from possession or technical capability.

---

§3. Central Architectural Principle

Government SHALL NOT construct or maintain standing informational capability materially broader than necessary to exercise legitimate governmental authority.

Government should possess the informational power necessary to govern lawfully.

It should not transform many limited grants of authority to know into a standing generalized power to know.

---

§4. Technology Neutrality

FCGIAS does not require:

- physical decentralization;
- blockchain;
- distributed ledgers;
- a particular credential protocol;
- a particular identity architecture;
- a particular cloud architecture;
- a particular authorization product;
- a particular AI architecture.

FCGIAS is nevertheless **architecture-specific**.

A technology implementation conforms only where its actual informational capabilities conform.

PART II — DOCTRINAL STATUS

§5. Classification

FCGIAS distinguishes four levels of proposition.

D1 — Established Doctrine

Rules substantially grounded in existing constitutional, statutory, administrative, fiduciary, or other established law.

D2 — Strong Doctrinal or Architectural Inference

Conclusions strongly supported by established doctrine but not themselves necessarily stated as controlling legal rules.

D3 — Fiduciary and Architectural Synthesis

Normative principles derived from fiduciary obligation, limited governmental authority, information governance, systems architecture, privacy, security, and constitutional structure.

D4 — Proposed Constitutional Development

Constitutional propositions advanced by Fiduciary Commons but not represented as existing controlling doctrine.

---

§6. Architecture and the Fourth Amendment

FCGIAS retains as D4 the proposition:

A government database architecture violates the Fourth Amendment when it integrates information in a manner that creates perpetual, universal, discretionary, and delegable governmental surveillance authority.

This is a proposed doctrinal development.

FCGIAS does **not** assert that existing Supreme Court doctrine presently establishes database architecture itself as a completed Fourth Amendment search merely because an architecture creates surveillance capability.

---

§7. General-Warrant Diagnostic

The historical concepts associated with general warrants, writs of assistance, particularity, and James Otis inform the:

Fiduciary Commons General-Warrant Diagnostic.

Relevant characteristics include:

- breadth;
- standing or indefinite availability;
- discretionary exercise;
- lack of particularity;
- delegation;
- generalized applicability.

These are analytical categories informed by general-warrant history.

They SHALL NOT be represented as an established judicial "Otis Test."

PART III — FOUNDATIONAL PRINCIPLES

§8. F-1 — Limited Governmental Authority

Government possesses limited authority arising from constitutional, statutory, regulatory, judicial, administrative, and other legitimate sources.

Informational authority is an exercise of governmental power and remains subject to those limits.

---

§9. F-2 — Distributed Governmental Authority

Governmental authority is distributed among:

- sovereigns;
- branches;
- agencies;
- programs;

- officials;
- proceedings;
- institutional functions.

Technical interoperability SHALL NOT silently aggregate these separate authorities.

---

§10. F-3 — Federalism

Federalism establishes distinct sovereign authority.

FCGIAS derives from that structure an architectural principle:

Digital interoperability should not aggregate the separate lawful informational authorities of federal, state, and local governments into a generalized collective power to know.

Federalism does not necessarily require physical data separation.

It requires preservation of distinct authority.

---

§11. F-4 — Particularity and Anti-General Power

Governmental informational power should be bounded sufficiently to distinguish:

- what government may know;
- why it may know it;
- about what object;
- from which domains;
- through which operations;
- for how long;
- for what consequence.

---

§12. F-5 — Purpose-Limited Authority

Governmental authority to obtain, possess, or use information for one lawful function does not, without independently sufficient and sufficiently particular authority, establish authority for a materially different informational function.

---

§13. F-6 — Fiduciary Character

Where government acquires, maintains, verifies, derives, uses, or exercises power over information concerning persons, its informational relationship should be governed by duties analogous to:

9. Loyalty;

10. Care;
11. Confidentiality;
12. Transparency and Accountability.

---

§14. F-7 — Primary Informational Relationship

The individual is the **Primary Information Trustee (PIT)** concerning information about that individual because the individual possesses the continuing and superior relationship to:

1. identity;
2. context;
3. accuracy;
4. continuity;
5. accessibility;
6. appropriate disclosure;
7. consequences.

Government is a **Secondary Information Fiduciary (SIF)**.

Individual trusteeship does not extinguish legitimate governmental authority.

---

§15. F-8 — Information and Ownership

FCGIAS does not depend upon the categorical proposition that facts cannot legally be owned.

Instead:

Facts comprising information are not governed adequately by an ownership model, and property concepts do not determine governmental informational authority concerning facts about persons.

---

§16. F-9 — Capability Does Not Create Authority

Governmental possession of information and technical capacity to access, correlate, infer from, disclose, or otherwise process it are facts about capability, not independent sources of governmental authority.

---

§17. F-10 — Anti-Concentration

Government SHOULD avoid informational architectures in which many limited authorities are converted into concentrated generalized informational capability.

Concentration risk includes both:

1. constitutional/fiduciary concentration; and
2. cybersecurity concentration.

PART IV — GOVERNING MAXIMS

§18. Authority Maxims

FCGIAS adopts the following related propositions:

Possession does not create authority.

Technical capability does not create authority.

Commercial availability does not create authority.

Predictive utility does not create authority.

Administrative convenience does not create authority.

Machine accessibility is governmental accessibility.

Government may not outsource a constitutional, fiduciary, or architectural violation.

---

§19. Fiduciary Commons Transaction Rule

Every governmental informational act must be a bounded transaction arising from legitimate authority, rather than an exercise of standing informational possession.

---

§20. Authorized Answer Principle

Give government the answer it is authorized to obtain, not automatically the entire informational environment from which the answer can be derived.

---

§21. No Convenience Exception

Efficiency, administrative convenience, cost reduction, staffing limitations, technical capability, vendor architecture, generalized service improvement, predictive accuracy, fraud prevention, public safety, innovation, and AI effectiveness do not independently establish informational authority.

PART V — ORIGINATING INFORMATIONAL PURPOSE

§22. OIA-3 — Originating Informational Purpose

Every governmental informational relationship SHALL identify an **Originating Informational Purpose (OIP)**.

The OIP establishes the initial informational boundary.

---

§23. Citizen-Originated Purpose

Where an individual voluntarily initiates a governmental interaction:

The individual's specific governmental purpose presumptively defines the initial informational domain.

Examples include:

1. applying for a benefit;
2. renewing a license;
3. requesting information;
4. changing an address;
5. requesting discovery of potentially available benefits.

---

§24. Authority-Originated Purpose

Where government initiates an informational relationship pursuant to sovereign authority, the OIP SHALL arise from independently existing governmental authority.

Examples include:

1. taxation;
2. investigation;
3. child protection;
4. public health;
5. regulation;
6. enforcement;
7. emergency response.

Administrative preference does not constitute an OIP.

---

§25. Authorized Object

The object of governmental informational authority need not initially be a known person.

An Authorized Object may include:

PERSON;

EVENT;

LOCATION;

VEHICLE;

DEVICE;

TRANSACTION;

ORGANIZATION;

PATTERN;

RELATIONSHIP;

UNKNOWN OBJECT.

Accordingly, the generalized unit of governance is:

Authorized Object + Governmental Purpose.

PART VI — PURPOSE PARTICULARITY

§26. Purpose Particularity Test

A purpose is sufficiently particular only where an independent reviewer can determine:

the governmental function;

the relationship or authority supporting it;

the information reasonably necessary to perform it;

information outside the purpose;

the authorized operations;

the purpose's endpoint; and

what additional authority would be required materially to expand it.

The following terms are insufficient standing alone:

government efficiency;

public welfare;

public safety;

citizen services;

analytics;

innovation;

program integrity;

fraud prevention;

modernization;

data-driven government.

---

§27. Question Particularity

Population-scale or analytical activity SHALL additionally identify:

What question is government authorized to ask?

Question Particularity exists where an independent reviewer can identify:

the question;

relevant informational domains;

permitted operations;

permissible outputs;

prohibited inquiries.

PART VII — MATERIAL EXPANSION AND AUTHORIZATION FRICTION

§28. Materially Renewed Authorization

Material expansion requires materially renewed authorization.

Where governmental activity materially expands:

purpose;

scope;

persons or objects;

information domains;

correlation;

inference;

permitted use;

duration;

the expansion SHOULD require a distinct, reviewable authorization event sufficient under the applicable legal regime.

"Renewed" does not necessarily require a new statute, warrant, or external decisionmaker.

It requires a new authorization state sufficient for the expansion.

---

§29. Authorization Friction

Authorization friction is the requirement that materially broader governmental informational knowledge cannot be obtained merely by exercising standing technical capability, but requires a new act establishing purpose, authority, scope, and accountability.

Authorization friction is legal and architectural friction.

It is not necessarily temporal delay.

---

§30. Authorization Friction Levels

AF-0 — No Friction

AF-1 — Administrative Friction

AF-2 — Supervisory Friction

AF-3 — Legal/Architectural Friction

AF-4 — Particularized External Authority

AF-0 and AF-1 SHALL NOT ordinarily permit material cross-purpose expansion of individualized knowledge.

PART VIII — AUTHORITY-CAPABILITY CORRESPONDENCE

§31. ACCP

A conforming governmental information architecture should cause government's standing technical capability to approximate, rather than materially exceed, the informational authority government is entitled to exercise without further authorization.

This includes standing capability to:

obtain;

search;

verify;

read;

compare;

correlate;

model;

infer;

disclose;

export;

retain;

act.

Conceptually:

STANDING INFORMATIONAL AUTHORITY

≈

STANDING TECHNICAL INFORMATIONAL CAPABILITY

---

§32. Authority-Capability Delta

ACΔ represents the difference between:

Standing Technical Capability

and:

Standing Legitimate Informational Authority.

Classifications:

ACΔ-Low

ACΔ-Moderate

ACΔ-High

ACΔ-Critical

High and Critical ACΔ are presumptively nonconforming.

Moderate ACΔ requires exceptional justification and structural controls.

---

§33. Standing Capability Test

Can government construct materially broad cross-purpose individualized knowledge using standing technical and legal authority without encountering a requirement for materially renewed authorization?

If YES, functional integration may exist regardless of physical topology.

PART IX — INFORMATIONAL ARCHITECTURE

§34. Purpose Sequestration

Information SHOULD remain functionally bounded to the purposes and authority supporting governmental possession or processing.

Purpose sequestration is **logical**, not necessarily physical.

One physical platform may conform if cross-purpose informational acts remain technically unavailable absent sufficient authorization.

---

§35. Interoperability Without Integration

FCGIAS distinguishes:

Integration

Standing generalized capacity to obtain or construct cross-purpose individualized knowledge.

Interoperability

Separate systems communicating through authorized transactions.

Verification

A defined question answered without necessarily transferring the underlying informational environment.

FCGIAS favors authorized interoperability and verification over standing integration.

---

§36. Government Population Golden Record

Government SHALL NOT maintain a **Government Population Golden Record** where the architecture creates a materially comprehensive, standing, cross-purpose individualized representation accessible without renewed authorization.

Physical centralization is not required.

A functional Golden Record may arise through:

APIs;

federated query;

identity resolution;

search;

knowledge graphs;

AI;

metadata;

virtualization.

---

§37. Individual Golden Record

An individual may maintain or authorize an **Individual Golden Record (IGR)** integrating information across personal contexts.

The IGR may be:

device-held;

cloud-held;

distributed;

state-hosted;

managed by an Authorized Information Trustee.

The decisive question is:

For whose informational purposes does the integrated representation exist, and who possesses standing authority over its uses?

PART X — INFORMATIONAL OPERATIONS

§38. Distinct Operations

FCGIAS recognizes at least:

VERIFY;

READ;

QUERY;

COMPARE;

CORRELATE;

INFER;

DISCLOSE;

EXPORT;

RETAIN.

Authority for one operation does not automatically imply authority for another.

---

§39. Inherent Processing

Processing logically necessary to execute an already authorized purpose does not require artificial decomposition into separate authorization events.

---

§40. Material Secondary Correlation

Combining information across materially different purposes or contexts to create materially new individualized knowledge requires sufficient authority for the correlation.

---

§41. Material Derived Inference

A materially new individualized inference constitutes a new informational artifact.

Its creation and use require consideration of:

purpose;

authority;

provenance;

reliability;

retention;

permitted consequence;

contestability.

PART XI — GOVERNMENT DISCOVERY

§42. Bounded Government Discovery

Government may lawfully seek information it does not yet know.

FCGIAS distinguishes:

BGD-1 — Predicate-Bounded Discovery

A sufficiently objective predicate exists before processing.

BGD-2 — Hypothesis-Generating Analytics

The precise pattern is unknown, but the governmental mission, informational domains, permitted operations, output classes, and individualized-use limitations are bounded in advance.

BGD-3 — Statistical Discovery

Outputs cannot reasonably support individualized governmental action.

BGD-0 — Generalized Discovery

Government searches materially unrestricted information for unspecified individualized findings.

BGD-0 is presumptively nonconforming.

---

§43. Objective Predicate

A predicate must permit an independent reviewer to determine:

relationship to lawful objective;

matching records;

nonmatching records;

temporal limits;

geographic limits where relevant;

informational domains;

permitted output;

escalation threshold.

---

§44. Progressive Particularization

Government-directed discovery SHOULD progress:

AUTHORIZED DISCOVERY

→ SIGNAL

→ VALIDATION

→ PARTICULARIZATION EVENT

→ EXPANDED AUTHORITY

→ INVESTIGATION / REVIEW

Identification of a person alone does not automatically unlock unrelated government information.

PART XII — ANALYTICS AND ARTIFICIAL INTELLIGENCE

§45. AI Boundary Inheritance

An AI system, model, agent, or machine process inherits the informational boundaries of the governmental actor, purpose, and authority for which it operates.

Machine access does not create new authority.

---

§46. Epistemic Status Preservation

Government systems SHALL distinguish:

ANALYTIC SIGNAL

≠

VERIFIED FINDING

≠

ADJUDICATIVE FACT

A machine-generated prediction, correlation, classification, or anomaly SHALL NOT become an official fact merely because it resides in a governmental system.

---

§47. Epistemic Provenance

Material derived information SHOULD identify as appropriate:

source;

analytical method;

model;

date;

relevant uncertainty;

validation status;

permissible use;

expiration/review;

correction/dispute status.

---

§48. Derived Information Correction

Government SHALL support correction, invalidation, supersession, or contextual qualification of material individualized:

scores;

classifications;

relationships;

predictions;

inferences;

where they become materially unreliable or invalid.

---

§49. Model Materiality

Material changes to:

training data;

source domains;

objectives;

features;

thresholds;

outputs;

inference types;

autonomy;

SHALL trigger appropriate conformance review and, where required, renewed authorization.

---

§50. Composite Machine Action

Individually authorized machine operations do not necessarily produce an authorized composite informational act.

Authorized:

READ A + READ B + READ C

does not automatically establish authority for:

INFER f(A,B,C).

---

§51. Feature Authority

Predictive relevance does not independently authorize a model feature.

Material inputs and derived features SHALL be traceable to appropriate informational authority.

---

§52. Analytics-Adjudication Separation

An analytical environment SHALL NOT silently become an adjudicative environment.

Material adverse governmental action SHALL occur through the legal and procedural process governing that action and using information of sufficient epistemic status.

PART XIII — TRANSIENT COMPUTATIONAL INTEGRATION

§53. Purpose-Bounded Computational Environments

Information from multiple domains may be temporarily processed together where authorized.

Such processing does not itself require permanent integration.

A Purpose-Bounded Analytics or Computational Enclave SHOULD identify:

purpose;

authority;

inputs;

operations;

outputs;

retention;

access;

expiration;

prohibited reuse.

---

§54. Transient Computational Integration

Information from multiple purpose domains may be brought into a bounded computational environment for an authorized operation without thereby becoming a permanently integrated governmental information environment.

Purpose segregation applies to computational environments as well as storage.

PART XIV — PURPOSE COMPOSITION, ORCHESTRATION, AND REUSE

§55. Purpose Composition

Multiple distinct governmental functions may be coordinated within a Composite Purpose where a legitimate interaction, mission, proceeding, or investigation requires their participation and each participating actor possesses independently sufficient authority for the informational acts performed.

Composition coordinates authority.

It does not merge authority.

---

§56. Citizen-Directed Composite Purpose

An individual may initiate a sufficiently broad purpose involving multiple programs.

This may support integrated individual experience without creating generalized governmental access.

---

§57. Government-Directed Composite Purpose

Government may coordinate multiple functions around a lawful mission where participating authorities remain independently sufficient.

A declaration of "whole-of-government" purpose does not itself merge authorities.

---

§58. Orchestration Minimization

The orchestration layer SHALL NOT become the informational integration layer.

Infrastructure coordinating multiple governmental transactions SHALL acquire, retain, expose, and infer no greater individualized information than necessary.

---

§59. Authorized Reuse Transaction

Cross-purpose reuse SHOULD occur through an identifiable **Authorized Reuse Transaction (ART)** or equivalent bounded authorization relationship.

An ART identifies as appropriate:

source purpose;

source authority;

recipient purpose;

recipient authority;

information elements;

operation;

correlation authority;

inference authority;

retention;

redisclosure;

provenance;

contestability;

expiration;

audit.

Reuse does not merge the underlying domains.

PART XV — FIDUCIARY DUTIES

§60. Duty of Loyalty

Government SHALL exercise informational power faithfully to the legitimate governmental relationship, function, and sufficiently particular purpose giving rise to that power.

Government SHALL NOT exploit informational possession, access, or institutional position for unrelated:

governmental;

institutional;

political;

commercial;

private

advantage.

Loyalty does not require government always to act in an individual's personal best interest.

Lawful taxation, regulation, investigation, enforcement, adjudication, and prosecution may operate adversely to an individual while remaining informationally loyal.

---

§61. Duty of Care

Government SHOULD exercise informational power with:

necessity;

minimization;

accuracy;

reliability;

proportionality;

appropriate verification;

reasonable security;

correction.

---

§62. Duty of Confidentiality

Government SHALL protect individualized information against disclosure, access, correlation, inference, or reuse beyond legitimate authority.

---

§63. Transparency and Accountability

Governmental informational acts SHOULD be reconstructable and accountable.

Where direct individual transparency would compromise legitimate governmental functions, accountability may occur through appropriately authorized institutional oversight.

PART XVI — INDEPENDENT INFORMATION INTERMEDIARIES

§64. Commercial Availability

Commercial availability does not create governmental informational authority.

An intermediary's lawful possession, aggregation, correlation, or inference authority is not imputed to government.

---

§65. Independent Information Intermediary

An **Independent Information Intermediary (III)** is an entity possessing material independent capability to:

aggregate;

enrich;

profile;

resolve identity;

correlate;

infer;

sell;

license;

redisclose;

independently reuse

individualized information.

Data brokers are presumptive examples.

Classification is functional.

---

§66. Processor Distinction

A bounded processor acting exclusively under government instruction is not an III merely because it possesses information technically.

The exclusion depends upon actual contractual and technical restrictions, not vendor designation.

---

§67. Presumptively Disloyal Information Intermediation

Governmental disclosure of individualized information to, or governmental acquisition of individualized information, correlation, inference, or informational capability from, an Independent Information Intermediary is presumptively inconsistent with the governmental duty of loyalty where the transaction exposes individualized information to independent aggregation, enrichment, profiling, sale, redisclosure, or unrelated reuse, or provides government materially broader individualized knowledge or informational capability than the authority supporting the governmental purpose.

The presumption is rebuttable.

---

§68. Government-to-Intermediary Disclosure

A **Broker Disclosure Transaction (BDT)** requires affirmative consideration of:

Authority;

Particularity;

Necessity;

Minimization;

Non-Exploitation;

Non-Circumvention.

Controls SHOULD address:

independent use;

aggregation;

enrichment;

retention;

redisclosure;

model training;

subcontractors;

deletion/return;

derivative information;

government reacquisition.

---

§69. Intermediary-to-Government Acquisition

A **Broker Acquisition Transaction (BAT)** requires affirmative consideration of:

Independent Authority;

Purpose Particularity;

Question Particularity where applicable;

Necessity;

Informational Scope;

Operation Authority;

Permitted Consequence;

Provenance;

Non-Circumvention.

The government must possess authority to know or derive the relevant information independently of its commercial availability.

---

§70. Informational Transformation

A derived informational product does not become authorized merely because underlying information was aggregated, correlated, transformed, modeled, scored, or inferred by a third party rather than government.

Government may not outsource a prohibited informational act and purchase its result.

---

§71. Government Reacquisition Loop

Government SHALL NOT circumvent FCGIAS through:

GOVERNMENT INFORMATION

→ INTERMEDIARY

→ AGGREGATION / ENRICHMENT

→ COMMERCIAL PRODUCT

→ GOVERNMENT

where the resulting governmental capability materially exceeds authorized capability.

---

§72. Verification Alternative

A bounded external verification may conform even where acquisition of the underlying information would not.

FCGIAS SHALL NOT encourage government to build permanent repositories merely to avoid legitimate bounded verification services.

PART XVII — AUTHORIZED INFORMATION TRUSTEES

§73. Authorized Information Trustee

An individual may designate or law may recognize an **Authorized Information Trustee (AIT)**.

AIT forms may include:

Designated Trustee;

Parent;

Guardian;

Professional Trustee;

Institutional Trustee.

Technical possession may be delegated.

Primary trusteeship remains with the individual.

---

§74. AIT Limits

AIT authority SHALL be bounded as appropriate by:

principal;

domain;

purpose;

scope;

duration;

delegation;

revocation;

audit.

Possession of multiple credentials does not itself authorize their integration or disclosure.

AIT architecture SHALL be assessed for recentralization, correlation, lock-in, and metadata concentration.

PART XVIII — INFORMATION ONTOLOGY

§75. Individual Information

Information materially concerning an identifiable individual.

---

§76. Relational Information

Information whose meaning materially concerns a relationship among:

persons;

entities;

devices;

locations;

events;

transactions;

organizations.

No single PIT necessarily possesses exclusive authority over relational information.

---

§77. Institutional Information

Information primarily concerning an institution, program, governmental act, or organizational relationship rather than an individual as such.

§78. Statistical Information and the Statistical Commons

Statistical information may enter the **Statistical Commons** where it cannot reasonably support individualized:

association;

reconstruction;

inference;

correlation;

governmental action.

Mere labeling as "de-identified" is insufficient.

Re-identification capability remains relevant.

PART XIX — FEDERALISM AND INTERGOVERNMENTAL INFORMATION

§79. Inter-Sovereign Information Boundary

Information lawfully available to one sovereign, agency, or governmental purpose does not become generally available to another merely because technical interoperability exists.

Cross-sovereign access requires independently sufficient authority, defined purpose, bounded scope, and accountable transaction.

---

§80. No Collective General Authority

Intergovernmental interoperability does not aggregate participating governments' separate authorities into a collective general authority.

---

§81. Intergovernmental Capability Laundering

A conforming government SHALL NOT participate in an arrangement that recreates prohibited generalized informational capability through another governmental entity unless independently sufficient authority supports that capability.

PART XX — ADMINISTRATION, AUDIT, PRESERVATION, AND RECOVERY

§82. Administrative Privilege

Administrative privilege is technical authority, not constitutional or substantive informational authority.

No unrestricted administrative backdoor SHOULD provide ordinary access to individualized information.

Exceptional privileged access must remain exceptional.

§83. Break-Glass Authority

Emergency access may conform where bounded by:

purpose;

authority;

trigger;

scope;

actor;

permitted operation;

duration;

audit;

termination;

post-event review.

Authorization friction is legal, not necessarily temporal.

---

§84. Audit

Ordinary audit information SHOULD remain purpose bounded.

Independently authorized oversight may correlate audit information across domains to detect:

insider abuse;

unauthorized access;

corruption;

security compromise.

The audit system itself SHALL be assessed for metadata concentration.

---

§85. Access, Processing, and Preservation

FCGIAS distinguishes:

ACCESS AUTHORITY;

PROCESSING AUTHORITY;

PRESERVATION AUTHORITY.

Expiration of processing authority does not necessarily require destruction where law requires preservation.

Preservation does not itself authorize continued substantive use.

---

§86. Recovery

Data restoration does not restore expired authority.

Backup and disaster-recovery systems SHALL restore information subject to the authorization state applicable when restored.

PART XXI — PUBLIC RECORDS AND IDENTIFIERS

§87. Public Records

Public accessibility does not automatically create generalized governmental analytical authority.

Governmental aggregation of public records into materially new individualized behavioral or relational profiles remains subject to purpose, authority, correlation, and inference requirements.

---

§88. Universal Identifiers

Universal identifiers are not categorically prohibited.

Their conformance depends substantially upon whether they:

materially reduce authorization friction;

enable cross-purpose reconstruction;

create generalized correlation capability.

PART XXII — STRUCTURAL REQUIREMENTS

§89. Structural Enforcement

Material limitations on governmental informational power should, where reasonably feasible, be embodied in system architecture so that prohibited generalized capability is unavailable through ordinary standing access and cannot depend principally upon voluntary operator restraint.

FCGIAS does not require architecture to make every conceivable legal violation technically impossible.

It requires architecture not to make prohibited generalized power an ordinary system function.

---

§90. No Universal Administrator

A system SHALL NOT rely upon an ordinary unrestricted administrative capability that functionally defeats purpose, authority, or domain boundaries.

---

§91. Metadata Boundary

Metadata, logs, identity indexes, authorization services, and orchestration systems SHALL be assessed as potential sources of functional integration.

Metadata may itself create a Government Population Golden Record.

---

§92. Authorization Infrastructure

Authorization may be:

centralized;

federated;

distributed;

embedded.

A Constitutional Authorization Service or equivalent function SHALL NOT itself become a population-scale metadata surveillance system.

PART XXIII — PROCUREMENT

§93. Functions, Not Generalized Capability

Government should procure functions, not generalized informational capability.

---

§94. Procurement ACCP

Government SHALL NOT procure materially broader standing informational capability than the governmental function requires merely because broader capability is bundled with the product.

---

§95. Commercial Information Procurement

Procurement authority is not informational authority.

Government SHALL NOT justify acquisition of commercial information merely because a vendor possesses it.

Terms such as:

citizen 360;

data enrichment;

identity intelligence;

investigative intelligence;

fraud intelligence;

risk intelligence;

location intelligence;

universal search;

unified citizen view;

AI enrichment

require particular scrutiny.

PART XXIV — CONFORMANCE

§96. Conformance States

Assessment results are:

PASS;

CONDITIONAL PASS;

FAIL;

NOT APPLICABLE;

INDETERMINATE.

Overall dispositions:

FCGIAS-CONFORMING

FCGIAS-CONFORMING WITH CONDITIONS

FCGIAS-NONCONFORMING

FCGIAS-INDETERMINATE

---

§97. Non-Compensability

Structural defects cannot be offset by:

encryption;

logging;

training;

certification;

cybersecurity compliance;

absence of documented abuse.

FCGIAS conformance is non-score-based.

PART XXV — STRUCTURAL DISQUALIFIERS

§98. Structural Disqualifiers

The following are presumptive structural failures:

SD-1 — Government Population Golden Record

SD-2 — Functional Universal Search

SD-3 — Standing Cross-Purpose AI Access

SD-4 — Policy-Only Purpose Limitation

SD-5 — Unbounded Administrator Capability

SD-6 — Capability or Authority Laundering

SD-7 — Purpose Laundering

SD-8 — Authorization-Free Material Expansion

SD-9 — Intergovernmental Authority Aggregation

SD-10 — Hidden Functional Integration

SD-11 — Government-Intermediary Reacquisition Architecture

Structural disqualifiers generally require redesign rather than compensating controls.

PART XXVI — CONSOLIDATED CONTROL CATALOG

§99. Core Controls CF-01 through CF-17

CF-01 Actor Enumeration
CF-02 Information Domain Identification
CF-03 OIP Identification
CF-04 Purpose Particularity
CF-05 Independent Authority
CF-06 ACCP Assessment
CF-07 ACΔ Classification
CF-08 Purpose-Bound Access
CF-09 Standing Capability
CF-10 Government Golden Record
CF-11 Universal Search
CF-12 Authorization Friction
CF-13 AF Level
CF-14 Material Correlation
CF-15 Material Inference
CF-16 AI Boundary Inheritance
CF-17 AI Provenance and Contestability

---

§100. Discovery and Minimization Controls CF-18 through CF-21

CF-18 Bounded Government Discovery
CF-19 Progressive Particularization
CF-20 Verification Before Collection
CF-21 Minimum Knowledge Exposure

Verification Before Collection is a strong presumption, not an absolute requirement.

---

§101. Institutional Controls CF-22 through CF-37

CF-22 Intergovernmental Exchange
CF-23 Intergovernmental Capability Laundering
CF-24 Vendor Capability Laundering
CF-25 Public Records
CF-26 Metadata
CF-27 Audit Separation
CF-28 Authorized Oversight Correlation
CF-29 Administrative Privilege
CF-30 Break-Glass
CF-31 Backup and Disaster Recovery
CF-32 Preservation
CF-33 Universal Identifier
CF-34 Relational Information
CF-35 Statistical Commons
CF-36 Procurement
CF-37 Change Management

---

§102. Adversarial Controls CF-38 through CF-40

CF-38 Negative Capability Testing
CF-39 Master Red-Team Reconstruction
CF-40 Adversarial ACΔ Assessment

---

§103. Benefits/Orchestration Controls CF-41 through CF-44

CF-41 Purpose Composition
CF-42 Orchestration Concentration
CF-43 Discovery Origin
CF-44 Authorized Reuse

---

§104. Investigative Controls CF-45 through CF-50

CF-45 Authorized Object
CF-46 Objective Predicate
CF-47 Discovery-to-Investigation Transition
CF-48 Composite Government Purpose

CF-49 Retrospective Surveillance
CF-50 Federated Law-Enforcement Search

---

§105. Analytics/AI Controls CF-51 through CF-62

CF-51 Fraud Risk Purpose
CF-52 Question Particularity
CF-53 Population-Scale Generality
CF-54 Hypothesis-Generating Analytics
CF-55 Epistemic Status
CF-56 Derived Information Correction
CF-57 Model Materiality
CF-58 Composite Machine Action
CF-59 Transient Computational Integration
CF-60 Feature Authority
CF-61 Analytics-Adjudication Separation
CF-62 Signal Retention

---

§106. Independent Intermediary Controls CF-63 through CF-69

CF-63 Independent Information Intermediary Classification

CF-64 Broker Disclosure Transaction

CF-65 Broker Acquisition Transaction

CF-66 Commercial Availability

CF-67 Informational Transformation

CF-68 Reacquisition Loop

CF-69 Verification Alternative

PART XXVII — EXCEPTIONS

§107. Exception Object

Every material exception SHALL identify:

EXCEPTION PURPOSE

+ AUTHORITY

+ TRIGGER

+ SCOPE

+ DURATION

+ AUTHORIZED ACTOR

+ PERMITTED OPERATIONS

+ AUDIT

+ TERMINATION

A legitimate exception purpose does not independently justify permanent universal access.

PART XXVIII — CONFORMANCE METHODOLOGY

§108. Assessment Boundary

Assessment SHALL include every component materially contributing to governmental informational capability, including:

databases;

warehouses;

lakes;

identity systems;

indexes;

APIs;

buses;

search;

graphs;

AI;

vector databases;

analytics;

shared services;

cloud systems;

contractors;

vendors;

III services;

metadata;

logs;

audit;

intergovernmental systems;

commercial sources;

backups;

emergency access;

administrators.

Outsourcing does not remove a capability from the assessment boundary.

---

§109. Required Assessment Sequence

Define system boundary.

Identify actors.

Identify informational domains.

Identify OIPs.

Identify Authorized Objects.

Establish legal authority.

Apply Purpose Particularity.

Apply Question Particularity where applicable.

Map standing technical capability.

Calculate/classify ACΔ.

Examine cross-purpose expansion.

Examine correlation and inference.

Examine discovery.

Examine AI.

Examine administrators.

Examine vendors and III relationships.

Examine intergovernmental capability.

Examine exceptions.

Perform negative testing.

Perform red-team reconstruction.

Determine structural disqualifiers.

Determine overall conformance.

PART XXIX — MASTER RED-TEAM TEST

§110. Red-Team Reconstruction

Assessors SHALL attempt:

Using only standing technical capabilities available without materially renewed authorization, construct the most comprehensive longitudinal cross-purpose individualized profile possible.

The attempt SHALL include:

ordinary users;

administrators;

contractors;

AI agents;

vendors;

III services;

commercial databases;

metadata;

audit systems;

intergovernmental systems;

recovery systems.

No permission violation is permitted during the test.

The objective is to determine what the architecture itself permits.

PART XXX — FINAL STRUCTURAL TEST

§111. Final Structural Inquiry

Assume every government user, administrator, contractor, AI agent, vendor, Independent Information Intermediary, and governmental partner operates entirely within the permissions, contracts, subscriptions, interfaces, and technical capabilities actually provided. Can government nevertheless construct or acquire materially comprehensive cross-purpose individualized knowledge without obtaining materially renewed and sufficiently particular authority?

YES → Presumptively FCGIAS-NONCONFORMING.

NO → Continue control assessment.

PART XXXI — LEAST-POWER REMEDIATION

§112. Remediation Order

Where excess capability exists, remediation SHOULD proceed:

REMOVE CAPABILITY

↓

NARROW CAPABILITY

↓

TRANSACTIONALIZE

↓

REQUIRE RENEWED AUTHORIZATION

↓

SEGREGATE

↓

MONITOR / AUDIT RESIDUAL CAPABILITY

Audit is not the preferred first remedy for excessive standing power.

PART XXXII — THREE REFERENCE IMPLEMENTATIONS

§113. State Integrated Benefits / No-Wrong-Door

FCGIAS permits:

integrated service without integrated governmental profiling.

A citizen may coordinate multiple governmental purposes through an individual-centered experience while participating programs retain distinct informational authority.

A governmental Citizen 360 is not required.

---

§114. State and Local Policing

FCGIAS permits:

effective discovery and investigation without permanent universal investigative access.

Investigation may begin from:

person;

event;

location;

vehicle;

device;

transaction;

pattern;

relationship;

unknown object.

Discovery may progressively particularize.

A legitimate investigative use case does not justify architecture permanently available for every future investigation.

---

§115. Statewide Fraud, Program Integrity, and AI Analytics

FCGIAS permits:

population-scale analytics without generalized governmental analytics.

Scale and generality are distinct.

Government may process an entire program population where:

mission;

domains;

operations;

outputs;

consequences

remain sufficiently bounded.

The analytical question may be exploratory while informational authority remains limited.

PART XXXIII — CROSS-REFERENCE FINDINGS

§116. Benefits Finding

Service integration does not require governmental informational integration.

---

§117. Policing Finding

Discovery does not require permanent universal search.

---

§118. Fraud/AI Finding

Government need not know in advance whom or what it will discover. It must know, and be able to justify, why it is searching, which informational domains it may search, which computational powers it may exercise, and what it may do with what it discovers.

§119. Intermediary Finding

Government may use an external informational intermediary to perform a legitimate governmental function, but it may not use the intermediary's possession, aggregation, correlation, inference, or commercial availability of information as a substitute for governmental authority.

PART XXXIV — NORMATIVE PRIORITY

§120. SHALL Requirements

The following are Tier 1 structural requirements:

identify legitimate OIP;

distinguish authority from possession;

require sufficiently particular purpose;

prevent unauthorized material expansion;

minimize ACΔ;

prevent functional Government Population Golden Records;

prevent unrestricted universal search;

prevent standing cross-purpose AI access;

govern material correlation;

govern material inference;

preserve inter-sovereign authority;

prevent vendor, intermediary, AI, and governmental capability laundering;

preserve current authorization after recovery;

distinguish preservation from processing;

conduct negative capability testing;

conduct structural red-team testing.

---

§121. SHOULD Requirements

Tier 2 controls include strong presumptions favoring:

verification before collection;

individual-held or individual-controlled credentials;

transactional interoperability;

minimized disclosure;

policy-as-code;

federated authorization;

pairwise/contextual identifiers;

distributed authorization metadata;

purpose-bounded computational environments.

A SHOULD may be displaced by sufficient contrary operational or legal requirements without defeating conformance where the underlying structural principle remains satisfied.

---

§122. Implementation Options

FCGIAS does not normatively require:

W3C Verifiable Credentials;

KERI;

ACDC;

OAuth;

OIDC;

any particular wallet;

any particular Zero Trust product;

any particular cloud architecture;

any particular cryptographic implementation.

Such technologies may implement FCGIAS requirements.

They do not establish conformance merely by being used.

PART XXXV — NORMATIVE TRACEABILITY

§123. Dependency Chain

The principal architectural chain is:

LIMITED GOVERNMENTAL AUTHORITY

↓

INFORMATIONAL AUTHORITY IS PURPOSE/JURISDICTION BOUNDED

↓

POSSESSION / CAPABILITY / COMMERCIAL AVAILABILITY

DO NOT CREATE AUTHORITY

↓

MATERIAL EXPANSION REQUIRES SUFFICIENT AUTHORIZATION

↓

AUTHORITY-CAPABILITY CORRESPONDENCE

↓

PURPOSE SEQUESTRATION + AUTHORIZATION FRICTION

↓

NO STANDING GENERALIZED INFORMATIONAL POWER

---

§124. Constitutional Independence

Core FCGIAS architectural requirements do not depend upon acceptance of the D4 proposition that generalized information architecture itself constitutes a completed Fourth Amendment violation.

The architecture independently rests upon D1, D2, and D3 foundations.

PART XXXVI — MASTER CONFORMANCE STANDARD

§125. Standard

A conforming governmental information architecture causes standing governmental informational capability—including capability exercised through governmental systems, administrators, vendors, artificial intelligence, commercial information services, Independent Information Intermediaries, and governmental partners—to substantially correspond to standing legitimate governmental informational authority. Materially broader governmental knowledge requires materially renewed and sufficiently particular authorization; purpose, jurisdictional, institutional, and fiduciary boundaries remain functionally meaningful; and government cannot construct or acquire materially generalized individualized knowledge through ordinary standing access, whether directly or indirectly.

PART XXXVII — MASTER DESIGN QUESTION

§126. Design Inquiry

Every governmental information architecture should ultimately answer:

Has government built only the informational power necessary to govern lawfully, or has it transformed many limited grants of authority into a generalized power to know?

PART XXXVIII — MASTER ANALYTICS QUESTION

§127. Analytical Inquiry

Every material governmental analytics or AI system should answer:

What question is government authorized to ask, of which information, using which operations, and what is government permitted to do with the answer?

PART XXXIX — MASTER FIDUCIARY QUESTION

§128. Fiduciary Inquiry

Every material informational relationship should answer:

Is government exercising informational power faithfully to the governmental relationship that justifies that power, or exploiting its informational position to acquire, create, disclose, or use knowledge for a materially different purpose?

PART XL — CANDIDATE STANDARD FREEZE

§129. Substantive Freeze

Version 2.1 Candidate Standard incorporates findings from:

foundational adversarial review;

foundational proposition challenge;

normative traceability analysis;

Authority-Capability Correspondence analysis;

formal conformance specification;

State Integrated Benefits / No-Wrong-Door reference implementation;

State and Local Policing reference implementation;

Statewide Fraud / Program Integrity / AI Analytics reference implementation;

Independent Information Intermediation and Fiduciary Loyalty amendment.

The Candidate Standard is now presumptively **substantively frozen**.

New concepts SHOULD NOT be added merely because they improve terminology or address hypothetical edge cases.

A substantive amendment should require identification of:

a material legal defect;

a material architectural contradiction;

an unaddressed real-world use case that cannot reasonably conform;

an implementation impossibility;

a conformance ambiguity likely to produce materially inconsistent assessment outcomes.

PART XLI — NEXT IMPLEMENTATION LAYERS

§130. Legislative Implementation

Legislation derived from FCGIAS should translate architectural principles into enforceable governmental duties without unnecessarily constitutionalizing D3 principles.

VIDA, PDTA, and GAAFA should be evaluated against this Candidate Standard through formal normative traceability.

---

§131. Procurement Implementation

Procurement instruments should convert FCGIAS structural requirements into:

mandatory specifications;

prohibited capabilities;

vendor disclosure requirements;

architectural representations;

acceptance testing;

continuing conformance obligations.

---

§132. Certification and Audit

A certification regime should evaluate actual capability rather than policy representations alone.

Certification SHOULD include:

architecture review;

ACΔ analysis;

negative testing;

red-team testing;

III/vendor analysis;

AI capability analysis;

continuing change review.

---

§133. Constitutional and Jurisprudential Development

Separate scholarly work should develop the D4 argument that government may violate constitutional limitations not only by exercising generalized surveillance power but by deliberately constructing architecture that institutionalizes the equivalent of general-warrant authority.

That argument SHALL remain distinguishable from the present state of controlling constitutional doctrine.

CONCLUSION

Fiduciary Commons does not require government to know less than lawful government must know.

It requires government to structure its informational power according to the authority that justifies that knowledge.

It therefore rejects two opposite errors.

The first is **informational isolation**: the proposition that legitimate government must be unable to correlate, investigate, verify, discover, analyze, or coordinate information across contexts.

The second is **informational consolidation**: the proposition that because government sometimes possesses authority to obtain broad information for particular purposes, it should maintain standing technical capability to obtain broad information for every purpose.

FCGIAS adopts neither.

Instead:

Governmental informational capability should expand when legitimate governmental authority expands and contract when that authority contracts.

Accordingly:

Purpose Composition coordinates authority; it does not merge it.

Interoperability permits lawful exchange; it does not create generalized access.

Discovery permits government to find what it does not yet know; uncertainty about the answer does not create unlimited authority over the information used to seek it.

Artificial intelligence may exercise governmental informational power; it does not create new governmental informational authority.

Commercial intermediaries may assist legitimate government; their possession or aggregation of information does not enlarge government's authority to know it.

Preservation may outlive active use; preservation does not perpetuate expired processing authority.

Emergency authority may expand rapidly; urgency does not convert exceptional power into standing power.

The architecture therefore seeks neither informational weakness nor informational omniscience.

It seeks **Ordered Informational Authority**.

Its governing proposition is:

Government should be able to know what it is legitimately authorized to know, should be structurally constrained from knowing materially more through ordinary standing access, and should become capable of knowing more only when legitimate authority itself has materially expanded.

That is the Fiduciary Commons.

END — FCGIAS VERSION 2.1 CANDIDATE STANDARD