

# PERSONAL DATA TRUSTEESHIP ACT

PDTA Version 2.2

Clean Restated Legislative Candidate

*September 13, 2026*

*September 7, 2026*

## **An Act to Establish a Fiduciary Framework for Governmental Informational Authority, Protect Individual Liberty and Autonomy, Define Duties Arising from Governmental Possession and Use of Information, and Implement the Fiduciary Commons Government Information Architecture Standard**

Companion statute to the Verifiable Identity and Digital Autonomy Act (VIDA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA).

Be it enacted by the [Legislative Body] as follows:

### **Section 1. Short Title**

(a) This Act may be cited as the "Personal Data Trusteeship Act" or "PDTA."

### **Section 2. Legislative Findings and Purposes**

#### **(a) Findings**

The [Legislative Body] finds that:

- (1) Information concerning a natural person is inseparably connected to that person's identity, relationships, activities, choices, rights, obligations, and participation in civil society, and governmental informational practices can materially affect individual liberty, autonomy, security, reputation, opportunity, and equality before the law.
- (2) Property concepts do not adequately determine the lawful authority of government to obtain, possess, verify, access, query, compare, correlate, infer from, disclose, export, retain, or otherwise act upon information concerning a person.
- (3) Governmental possession of information does not itself establish governmental authority to use that information for every governmental purpose, and technical capability to access, combine, analyze, or infer from information does not itself create legal authority to exercise that capability.
- (4) Commercial availability of information does not itself create governmental informational authority, and government may not enlarge its lawful authority merely by acquiring information, informational products, correlations, inferences, or analytical capabilities from a private or governmental intermediary.
- (5) A natural person has a unique and continuing relationship to information concerning that person, including interests in its accuracy, context, integrity, confidentiality, appropriate use, accessibility, correction, continuity, and protection from misuse.

- (6) This relationship supports recognition of the individual as the Primary Information Trustee of information concerning that individual, without requiring the information itself to be characterized as property owned by the individual.
- (7) Government that obtains, possesses, processes, verifies, correlates, infers from, discloses, retains, or otherwise exercises informational power concerning a person acts as a Secondary Information Fiduciary and owes duties arising from the governmental relationship, lawful function, and informational authority supporting that power.
- (8) Governmental informational authority is limited by the Constitution, statutes, regulations, judicial orders, lawful administrative authority, jurisdiction, governmental function, and sufficiently particular purposes supporting the informational act.
- (9) Authority to perform one governmental informational act does not, without independently sufficient authority, establish authority to perform a materially different informational act.
- (10) Materially broader governmental informational power should require materially renewed and sufficiently particular authorization and should not arise merely from possession, administrative convenience, technical interoperability, predictive utility, commercial availability, or the existence of a generalized technical capability.
- (11) Government information architecture should cause Standing Technical Informational Capability to correspond to, and not materially exceed, Necessary Standing Informational Capability, which in turn must remain within Standing Legitimate Informational Authority.
- (12) Government should therefore avoid architectures that transform multiple limited grants of authority into standing generalized capability to construct materially comprehensive cross-purpose knowledge concerning persons through ordinary official access.
- (13) The constitutional history of prohibitions against general warrants demonstrates a longstanding commitment to particularity, bounded governmental authority, and protection against discretionary governmental power to search broadly without sufficiently particular justification.
- (14) Modern information systems can create functional equivalents of generalized governmental informational power through centralized databases, federated queries, application programming interfaces, identity resolution, universal search, metadata aggregation, knowledge graphs, artificial intelligence, commercial information services, or other mechanisms even when information is not physically maintained in a single repository.
- (15) Whether a governmental information architecture is lawful and fiduciary therefore depends upon the informational capability it creates and the authority governing that capability, not merely upon the physical location, ownership, security, encryption, or organizational arrangement of the underlying information.
- (16) The Fourth Amendment to the United States Constitution, the Constitution of [Enacting State], and the historical prohibition against general warrants provide important constitutional foundations for limiting generalized governmental informational power; this Act additionally establishes independent statutory fiduciary protections that do not depend upon a judicial determination that any particular information architecture constitutes a search or seizure under existing federal constitutional doctrine.
- (17) [Citation to State popular-sovereignty or social-compact provision] establishes that governmental power originates in and remains accountable to the people and supports imposing fiduciary obligations upon governmental exercise of informational power.

(18) [Citation to State inherent-rights provision] recognizes rights of persons existing independently of governmental creation and supports protection of individual informational autonomy against unauthorized governmental exploitation.

(19) [Citation to State search-and-seizure provision] independently protects against unreasonable or insufficiently particular governmental acquisition and use of information according to the text, history, and law of this State.

(20) Government legitimately performs functions that may be initiated by the individual, including applications for benefits, licenses, credentials, permits, and services, and functions initiated pursuant to independent governmental authority, including taxation, regulation, investigation, adjudication, enforcement, emergency response, public health, fraud detection, and protection of persons.

(21) Individual consent therefore constitutes an important source of authority in appropriate citizen-originated relationships but cannot serve as the exclusive legal basis for all legitimate governmental informational activity.

(22) Legitimate government may require interoperability, cross-domain analysis, discovery of previously unknown persons or patterns, and computation across multiple information domains; such activities must remain bounded by lawful purpose, sufficient authority, particularity, necessity, authorized informational operations, permitted consequences, accountability, and appropriate authorization transitions.

(23) Artificial intelligence, automated systems, contractors, vendors, commercial information services, and governmental partners may exercise informational capability on behalf of government but cannot independently enlarge the informational authority of the governmental function they serve.

(24) Fiduciary duties are most effective when material limitations upon informational power are implemented structurally, so that prohibited generalized capability is unavailable through ordinary standing access rather than dependent principally upon voluntary restraint after access has been granted.

(25) Effective protection requires enforceable rights, burdens of justification placed upon the governmental or secondary fiduciary exercising informational power, meaningful remedies, independent oversight, and architectural conformance requirements.

(26) Positive legal authorization is a necessary source of governmental authority where required by law, but broad authorization to perform a governmental function does not by itself establish that every informational capability technically useful to that function is legitimate in scope under this Act.

(27) Legitimate Informational Authority must be justified in both 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 degree of Purpose Divergence.

(28) The justification required for governmental informational power increases as the proposed informational act materially diverges from the Originating Informational Purpose, expands individualized or relational knowledge, increases governmental consequence, or creates durable or reusable standing capability.

(29) Legitimate authority is an outer ceiling on governmental informational power, not a procurement specification. Ordinary standing technical capability should not materially exceed the capability reasonably necessary to perform the legitimate standing governmental function.

(30) Where broader informational capability may legitimately become necessary only after a predicate, relationship, purpose, or authorization materially changes, architecture should make that broader capability available through the corresponding authorization transition rather than maintain it as unnecessary ordinary standing power.

#### **(b) Purposes**

The purposes of this Act are to:

- (1) establish a fiduciary legal framework governing governmental informational power;
- (2) recognize natural persons as Primary Information Trustees of information concerning themselves without making ownership of facts the basis of the protections established by this Act;
- (3) establish government and persons exercising governmental informational power as Secondary Information Fiduciaries;
- (4) require governmental informational acts to arise from legitimate authority and sufficiently particular purposes;
- (5) distinguish citizen-originated governmental purposes from authority-originated governmental purposes;
- (6) establish that possession, technical capability, commercial availability, predictive utility, and administrative convenience are not independent sources of governmental informational authority;
- (7) require materially renewed authorization when governmental informational capability materially expands;
- (8) impose fiduciary duties of loyalty, care, confidentiality, and transparency and accountability;
- (9) prevent the conversion of multiple bounded governmental authorities into standing generalized governmental informational power;
- (10) permit lawful governmental interoperability, verification, bounded discovery, investigation, analytics, fraud detection, and other legitimate functions without requiring generalized informational integration;
- (11) establish enforceable rights and remedies for violations of governmental informational fiduciary duties;
- (12) provide the legal superstructure for the technical architecture established by VIDA and the artificial-intelligence and automated-decision requirements established by GAAFA; and
- (13) require implementation consistent with the Fiduciary Commons Government Information Architecture Standard as adopted pursuant to this Act;
- (14) distinguish Positive Legal Authority from Legitimate Informational Authority and prevent broad legal authorization from operating as a conformance bootstrap;
- (15) require greater informational justification as governmental informational activity materially diverges from its Originating Informational Purpose; and
- (16) require ordinary Standing Technical Informational Capability to remain no broader than reasonably necessary for the legitimate standing governmental function.

## Section 3. Definitions

### (a-1) Trilogy Definition Precedence

For purposes of PDTA, VIDA, and GAAFA, the definitions in this section govern unless VIDA or GAAFA expressly defines a specialized term for the subject matter governed by that Act. A specialized definition supplements and, only to the extent expressly stated or necessarily required by the specialized provision, controls over the general PDTA definition. No specialized definition shall be construed to create Governmental Informational Authority by implication.

For purposes of this Act:

### (a) “Authorized Information Trustee”

“Authorized Information Trustee” or “AIT” means a natural person or legally cognizable entity lawfully authorized to exercise specified informational rights or responsibilities on behalf of a Primary Information Trustee, including a parent, guardian, designated representative, professional fiduciary, or institutional fiduciary, subject to the scope, purpose, duration, delegation, revocation, and accountability requirements applicable to that authorization.

### (b) “Authorized Informational Act”

“Authorized Informational Act” means an informational or computational operation supported by sufficient authority for the governmental purpose, Authorized Object, information domain, scope, duration, and permitted consequence involved. Authorized Informational Acts include, as applicable and without limitation: (1) VERIFY; (2) IDENTIFY; (3) AUTHENTICATE; (4) AUTHORIZE OPERATION; (5) READ; (6) QUERY; (7) COMPARE; (8) RESOLVE; (9) CORRELATE; (10) INFER; (11) CLASSIFY; (12) RANK; (13) SCORE; (14) PREDICT; (15) DISCLOSE; (16) EXPORT; (17) RETAIN; and (18) ACT UPON INFORMATION. A functionally equivalent operation is governed according to its actual informational capability and consequence. Authorization for one informational act does not by itself constitute authorization for another.

### (c) “Authorized Object”

“Authorized Object” means the person, event, location, vehicle, device, transaction, organization, pattern, relationship, unknown object, or other legally cognizable object to which a governmental informational purpose is directed. An Authorized Object need not be a known or identified person at the commencement of a lawful governmental inquiry.

### (d) “Authority-Originated Purpose”

“Authority-Originated Purpose” means an Originating Informational Purpose initiated by government pursuant to independently existing constitutional, statutory, regulatory, judicial, or other lawful governmental authority rather than at the request of an individual.

### (e) “Citizen-Originated Purpose”

“Citizen-Originated Purpose” means an Originating Informational Purpose arising when a natural person voluntarily initiates a governmental interaction to obtain, exercise, establish, verify, or protect a nonmandatory right, benefit, service, license, permit, credential, status, or other governmental function. The individual’s specific voluntary purpose presumptively establishes the initial informational boundary of the interaction and does not constitute generalized consent to materially unrelated governmental inquiry, correlation, inference, retention, disclosure, or reuse.

**(f) “Commercial Availability”**

“Commercial Availability” means that information, an informational product, an analytical result, an inference, or an informational capability is offered, licensed, sold, searchable, accessible, or otherwise available from a nongovernmental source. Commercial Availability is not an independent source of governmental informational authority.

**(g) “Functional Universal Search”**

“Functional Universal Search” means ordinary Standing Technical Capability permitting a Governmental Actor to formulate materially unconstrained individualized or relational queries across materially unrelated information domains without an authorization transition sufficient for the query performed.

**(h) “GAAFA”**

“GAAFA” means the Government Algorithmic Accountability and AI Fiduciary Act, as enacted and subsequently amended.

**(i) “Generalized Governmental Informational Power”**

“Generalized Governmental Informational Power” means Standing Technical Capability through which government may acquire or construct materially broad cross-purpose individualized or relational knowledge at official discretion without a separately sufficient authorization event establishing the purpose, authority, scope, informational operations, duration, and permitted consequence of that exercise.

**(j) “Government Agency”**

“Government Agency” means any executive department, agency, office, board, commission, authority, instrumentality, political subdivision, public corporation, or other governmental unit of [Enacting State] subject to this Act. A contractor, vendor, agent, service provider, or other nongovernmental person does not become a Government Agency merely because that person exercises Governmental Informational Power on behalf of a Government Agency. The application of this Act to the legislative and judicial branches is governed by Section 23.

**(k) “Government Population Golden Record”**

“Government Population Golden Record” means a governmental informational environment that permits ordinary Standing Technical Capability to obtain or construct a materially comprehensive cross-purpose individualized representation of persons. A Government Population Golden Record may exist through centralized storage or functionally through federated query, application programming interfaces, identity resolution, universal search, knowledge graphs, artificial intelligence, metadata aggregation, data virtualization, commercial information services, or other mechanisms.

**(k-1) “Composite Governmental Information Transaction”**

“Composite Governmental Information Transaction” means a functionally related sequence, combination, or orchestration of governmental informational acts, technical operations, disclosures, acquisitions, correlations, inferences, automated actions, or intergovernmental or Vendor-mediated steps that together perform or materially support a governmental function. The transaction shall be evaluated end-to-end according to its aggregate technical capability and the separately applicable purposes, authorities, Authorized Objects, information domains, informational operations, actors, duration, outputs, consequences, and authorization transitions. A Composite Governmental Information Transaction is an assessment and accountability unit

only. It does not merge, pool, transfer, or aggregate the separate Governmental Informational Authority, jurisdiction, Originating Informational Purpose, predicate, or permitted consequence of a participating actor, agency, program, or sovereign.

(k-2) "Exception Envelope"

"Exception Envelope" means the complete set of legally and operationally bounded conditions governing an exceptional or nonordinary governmental informational capability, including: (1) the exception purpose; (2) independently sufficient legal authority; (3) the triggering condition or predicate; (4) authorized actors or systems; (5) Authorized Objects or affected scope; (6) information domains; (7) permitted informational operations; (8) permitted governmental consequences; (9) duration or expiration; (10) logging, audit, and review; (11) termination conditions; and (12) any required post-use remediation, notice, or accountability. An Exception Envelope implements existing authority and does not itself create Governmental Informational Authority.

(k-3) "Responsible Government Agency"

"Responsible Government Agency" means the Government Agency designated or otherwise identifiable as the principal accountability and coordination locus for the governmental function or Composite Governmental Information Transaction at issue. Designation of a Responsible Government Agency assigns accountability and coordination responsibility only and does not transfer, enlarge, or aggregate Governmental Informational Authority, jurisdiction, custody, programmatic decisional authority, or ordinary technical access. Other participating Government Agencies, Vendors, and Governmental Actors retain the independent duties, authority limits, and liability applicable to their conduct.

(k-4) "Role Stacking"

"Role Stacking" means the circumstance in which the same natural person, Government Agency, Vendor, contractor, intermediary, system operator, or other legally cognizable entity occupies more than one statutory or functional role in the same or related governmental informational activity. Duties, restrictions, burdens, and accountability attach according to each role actually performed and are cumulative to the extent compatible. A person may not avoid an obligation applicable to one role by relying upon a different role occupied in the same transaction.

(k-5) "Trilogy Conformance Code"

"Trilogy Conformance Code" means the single public, version-controlled body of binding DTA conformance regulations, incorporated technical controls, authoritative crosswalks, and implementation classifications adopted under Section 25 to administer PDTA, VIDA, and GAAFA consistently. The Trilogy Conformance Code is an implementation and conformance instrument and does not independently create Governmental Informational Authority, substantive rights, exceptions, causes of action, or liability.

**(l) "Governmental Actor"**

"Governmental Actor" means an officer, employee, contractor, Vendor, agent, service provider, automated system, artificial intelligence system, or other person or system exercising Governmental Informational Power for or on behalf of a Government Agency. Inclusion of an automated or artificial intelligence system within this definition is solely for attribution of informational capability, architectural assessment, conformance, and responsibility. It does not confer legal personhood, capacity to hold Governmental Informational Authority, independent fiduciary status, or independent civil liability upon software.

(l-1) "Vendor"

"Vendor" means a contractor, subcontractor, licensor, provider, operator, host, service provider, cloud provider, model provider, application-programming-interface provider, or other nongovernmental person supplying, operating, maintaining, or materially supporting an information system, informational capability, identity service, analytical service, algorithmic, automated, or artificial-intelligence system or service, or material component for or on behalf of a Government Agency. Vendor status is determined by actual function and does not by itself make the Vendor a Government Agency.

**(m) "Governmental Informational Authority"**

"Governmental Informational Authority" means authority sufficient to support a governmental informational act under this Act. It includes the applicable Positive Legal Authority and is bounded by the governmental function, jurisdiction, Originating Informational Purpose, Authorized Object or predicate, information domain, authorized operation, necessity, duration, permitted consequence, and other substantive limitations imposed by this Act.

**(m-1) "Positive Legal Authority"**

"Positive Legal Authority" means authority arising from a constitution, statute, regulation within delegated authority, judicial process, lawful administrative authority, individual authorization where legally cognizable, emergency authority, or another legally sufficient source competent to authorize the governmental act at issue.

**(m-2) "Legitimate Informational Authority"**

"Legitimate Informational Authority" means governmental authority to obtain, verify, know, correlate, infer, disclose, retain, or act upon information that is justified in both 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 the degree of Purpose Divergence involved.

**(m-3) "Standing Legitimate Informational Authority"**

"Standing Legitimate Informational Authority" means the outer boundary of Legitimate Informational Authority that a Governmental Actor may exercise through ordinary standing governmental processes without a materially changed predicate, relationship, purpose, or Materially Renewed Authorization.

**(n) "Governmental Informational Power"**

"Governmental Informational Power" means governmental capability to obtain, verify, know, access, query, compare, correlate, infer, disclose, export, retain, or act upon information.

**(o) "Individual Information"**

"Individual Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or may reasonably support individualized knowledge concerning a natural person.

**(p) "Inherent Processing"**

"Inherent Processing" means processing, comparison, calculation, or inference that is reasonably necessary and logically inherent in carrying out an already authorized governmental informational act and that does not materially expand the governmental purpose, information domains, Authorized Object, individualized knowledge, or permitted consequence.

**(q) “Material or Materially”**

“Material” or “materially” means more than de minimis and reasonably capable of: (1) altering the scope of Governmental Informational Authority; (2) increasing individualized or relational governmental knowledge in a manner significant to the governmental purpose; (3) affecting a person’s rights, obligations, eligibility, status, liberty, opportunity, or governmental treatment; or (4) expanding Standing Technical Capability in a manner significant to the purposes of this Act. Materiality shall be evaluated in context and shall not depend solely upon the volume of information processed.

**(q-1) “Informational Justification Level”**

“Informational Justification Level” or “IJ Level” means the level of justification required under this Act according to the relationship between the proposed informational act and the Originating Informational Purpose, together with materiality, necessity, informational scope, consequence, duration, and standing capability.

**(q-2) “Purpose Divergence”**

“Purpose Divergence” means a material departure between the Originating Informational Purpose and a later governmental informational purpose, question, domain, operation, class of Authorized Objects, consequence, duration, or reusable standing capability. Divergence may occur within one agency, across agencies, across sovereigns, through a Vendor or intermediary, or through automated or artificial-intelligence processing.

**(r) “Material Derived Inference”**

“Material Derived Inference” means a prediction, classification, score, relationship, conclusion, or other informational artifact produced from existing information that materially expands what government knows or claims to know concerning an Authorized Object beyond information inherent in the authorized processing of the existing purpose.

**(s) “Material Expansion”**

“Material Expansion” means a change in governmental informational activity that materially broadens one or more of the following: (1) governmental purpose; (2) Authorized Object or class of Authorized Objects; (3) information domain; (4) category or amount of information; (5) informational operation; (6) correlation authority; (7) inferential authority; (8) duration or retention; (9) disclosure or recipient; (10) governmental consequence; or (11) Standing Technical Capability available without additional authorization.

**(t) “Material Secondary Correlation”**

“Material Secondary Correlation” means the combination, association, or comparison of information across materially distinct purposes, domains, relationships, or governmental contexts in a manner that creates or is reasonably capable of creating materially new individualized or relational governmental knowledge.

**(u) “Materially Renewed Authorization”**

“Materially Renewed Authorization” means a distinct and reviewable authorization event that is both legally sufficient under the applicable legal regime and substantively sufficient under this Act for the proposed Material Expansion. It shall establish, as applicable, Positive Legal Authority, legitimate governmental function, relationship or predicate, Originating Informational Purpose, Authorized Object, question, information domains, authorized operations, necessity, proportionality where applicable, permitted consequence, duration, accountability, Purpose

Divergence, and the applicable Informational Justification Level. Materially Renewed Authorization does not necessarily require the same form of authorization in every governmental context.

**(v) “Ordered Informational Authority”**

“Ordered Informational Authority” means 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.

**(w) “Originating Informational Purpose”**

“Originating Informational Purpose” or “OIP” means the sufficiently particular governmental purpose that establishes the initial boundary of informational authority for a governmental interaction or function. An OIP may be Citizen-Originated or Authority-Originated.

**(x) “Primary Information Trustee”**

“Primary Information Trustee” or “PIT” means the natural person possessing the primary informational relationship to Individual Information concerning that person. Primary Information Trusteeship does not depend upon ownership of the information and does not by itself displace lawful governmental authority or the lawful rights of other persons.

**(y) “Processing”**

“Processing” means an informational operation performed upon information, including obtaining, recording, organizing, structuring, accessing, querying, comparing, correlating, analyzing, inferring from, using, disclosing, transmitting, exporting, or otherwise manipulating information. For purposes of Section 18, Active Processing Authority, Retention Authority, and Preservation Authority are distinct forms of legal authority notwithstanding that retention or preservation may constitute processing under another law.

**(z) “Purpose Sequestration”**

“Purpose Sequestration” means the functional preservation of boundaries among governmental informational purposes such that information or capability available for one purpose is not ordinarily available for a materially different purpose without sufficient authority for the additional informational act. Purpose Sequestration may be implemented logically, physically, cryptographically, organizationally, transactionally, or through a combination of controls and does not require separate physical infrastructure where equivalent functional separation is achieved.

**(aa) “Question Particularity”**

“Question Particularity” means sufficient specification of an analytical, investigative, statistical, or computational governmental inquiry to permit an independent reviewer to determine: (1) what governmental question is being asked; (2) what information domains are relevant to the question; (3) what informational or computational operations are authorized; (4) what outputs may be produced; (5) what uses or governmental consequences may follow; and (6) what materially different questions or uses remain outside the authorization.

**(bb) “Relational Information”**

“Relational Information” means information materially concerning a relationship, association, interaction, transaction, network, household, organization, event, device, location, or pattern involving more than one person or legally relevant object. Relational Information shall not be treated as exclusively attributable to a single Primary Information Trustee merely because one person is identifiable within it.

**(cc) “Secondary Information Fiduciary”**

“Secondary Information Fiduciary” or “SIF” means: (1) a Government Agency exercising Governmental Informational Power concerning Individual Information or Relational Information; or (2) another person expressly made a Secondary Information Fiduciary by enacted law. A Vendor, contractor, agent, or service provider does not become a Secondary Information Fiduciary merely by contracting with or providing capability to government. Such persons remain subject to duties expressly imposed by law, procurement requirements, contract, agency principles where applicable, and Section 17.

**(dd) “Standing Technical Capability”**

“Standing Technical Capability” or “Standing Technical Informational Capability” means informational capability available to a Governmental Actor through ordinary existing permissions, interfaces, subscriptions, credentials, processes, or system functions without Materially Renewed Authorization.

**(dd-1) “Necessary Standing Informational Capability”**

“Necessary Standing Informational Capability” means the ordinary standing informational capability reasonably necessary to perform the legitimate standing governmental function, considering materially less informationally powerful architectures, transaction-specific or predicate-activated alternatives, Utility, Security, reliability, continuity, and the governmental consequences of under-capability. It shall remain within Standing Legitimate Informational Authority.

**(ee) “Statistical Information”**

“Statistical Information” means information that, considering available data, technology, linkages, and reasonably foreseeable means of analysis, cannot reasonably be used to identify a person or to support individualized association, correlation, inference, classification, or governmental action concerning a person.

**(ff) “VIDA”**

“VIDA” means the Verifiable Identity and Digital Autonomy Act, as enacted and subsequently amended.

## **Section 4. Primary Information Trusteeship**

**(a) Recognition**

A natural person is the Primary Information Trustee of Individual Information concerning that person.

### **(b) Nature of Trusteeship**

Primary Information Trusteeship: (1) arises from the individual's primary and continuing relationship to information concerning the individual; (2) does not depend upon a finding that facts or information constitute property owned by the individual; (3) recognizes the individual's legitimate interests in accuracy, context, integrity, confidentiality, appropriate use, accessibility, correction, continuity, and protection from unauthorized exploitation; (4) does not confer authority upon an individual to extinguish independently lawful governmental authority, the rights of another person, lawful preservation obligations, public-record obligations, or other legal interests merely because information concerns that individual; and (5) shall be construed consistently with the fiduciary, constitutional, and statutory limitations established by this Act.

### **(c) Individual Authorization**

Where a governmental informational act arises from a Citizen-Originated Purpose and no independent governmental authority requires otherwise, the Primary Information Trustee's informed and voluntary authorization may establish or define the scope of governmental informational authority.

### **(d) No Consent Fiction**

A Government Agency may not rely upon purported consent or authorization that is: (1) coerced; (2) materially conditioned upon an unrelated government benefit or service; (3) materially broader than the governmental interaction to which the person agreed; (4) obtained through deceptive or materially incomplete disclosure; (5) bundled with materially unrelated informational purposes; or (6) otherwise insufficient under this Act.

### **(e) Withdrawal**

Withdrawal of individual authorization terminates informational authority dependent solely upon that authorization prospectively, subject to: (1) independently sufficient governmental authority; (2) lawful preservation requirements; (3) completion of a legally required adjudicative, audit, enforcement, or records process; and (4) other obligations expressly established by law. Withdrawal does not retroactively invalidate informational acts lawfully completed while authorization existed.

### **(f) Statutory Character**

Primary Information Trusteeship and Secondary Information Fiduciary status under this Act are statutory informational relationships. They do not require: (1) creation of an express trust; (2) identification of a trust corpus; (3) transfer of legal or equitable title; (4) characterization of information or facts as property; or (5) satisfaction of formal requirements applicable to creation of a private trust. Common-law fiduciary and trust principles may inform interpretation of this Act only to the extent consistent with its text, purposes, and governmental context. Nothing in this Act shall be construed to create ownership of facts merely by using the terms "trustee," "trusteeship," or "fiduciary."

## **Section 5. Government as Secondary Information Fiduciary**

### **(a) Fiduciary Status**

A Government Agency becomes a Secondary Information Fiduciary when it exercises Governmental Informational Power concerning Individual Information or Relational Information.

#### **(b) Relationship, Not Possession Alone**

The fiduciary relationship established by this Act arises from governmental exercise of informational power and is not dependent upon: (1) ownership of the information; (2) execution of a contract; (3) acceptance of terms of service; (4) physical custody of a database; (5) whether the information is obtained directly from the Primary Information Trustee; (6) whether the information is obtained from another governmental entity; (7) whether the information is commercially available; (8) whether the information is generated through correlation, inference, or artificial intelligence; or (9) whether government accesses the information without retaining a permanent copy.

#### **(c) No Authority by Possession**

Governmental possession of information does not independently authorize any informational act concerning that information.

#### **(d) No Authority by Capability**

The existence of technical capability to perform an informational act does not independently authorize that act.

#### **(e) No Authority by Commercial Availability**

The lawful possession or commercial availability of information, an informational product, an inference, a score, a profile, an identity-resolution service, or another informational capability in the hands of a nongovernmental person does not independently establish governmental authority to acquire or use it.

#### **(f) No Authority by Intergovernmental Availability**

Information lawfully available to one Government Agency, governmental purpose, political subdivision, sovereign, or governmental partner does not become generally available to another merely because technical interoperability, information sharing, or institutional cooperation exists.

#### **(g) Vendors and Agents**

A Government Agency may not avoid or reduce an obligation imposed by this Act by delegating an informational act to a contractor, vendor, artificial intelligence system, service provider, intermediary, governmental partner, or other agent.

## **Section 6. Originating Informational Purpose and Governmental Informational Authority**

#### **(a) Originating Informational Purpose Required**

Every material governmental informational activity shall arise from an identifiable Originating Informational Purpose.

#### **(b) Citizen-Originated Purpose**

Where an individual voluntarily initiates a governmental interaction, the individual's specific purpose in seeking the governmental function presumptively defines the initial informational boundary. Government may obtain or use information reasonably necessary for that purpose, subject to this Act and other law. Government may not treat initiation of the interaction as generalized consent or authorization for materially unrelated inquiry, correlation, inference,

retention, disclosure, reuse, or another governmental purpose. Independently existing Authority-Originated Purposes remain available only on their own sufficient authority and justification.

#### **(c) Authority-Originated Purpose**

Government may initiate an informational activity without individual authorization where: (1) the activity arises from independently sufficient governmental authority; (2) the governmental purpose is sufficiently particular; (3) the information and informational operations are reasonably necessary and appropriately bounded to that purpose; (4) any predicate required by applicable law is satisfied; and (5) the informational activity otherwise complies with this Act.

#### **(d) Authorized Object**

A Government Agency shall identify the Authorized Object of a material informational activity at the level of particularity reasonably available at the relevant stage of the governmental function. An Authorized Object may initially be unknown where the government is lawfully authorized to discover the identity, relationship, event, transaction, pattern, or other object relevant to the governmental purpose.

#### **(e) Authority Follows Purpose**

Governmental informational authority shall be evaluated in relation to the purpose and governmental function supporting the informational act. Authority sufficient for one purpose does not, by possession or implication alone, establish authority for a materially different purpose.

#### **(f) Capability Does Not Enlarge Authority**

No Government Agency may construe interoperability, administrative access, database possession, contractual access, a vendor subscription, a commercial search capability, artificial intelligence capability, predictive usefulness, technical efficiency, or administrative convenience as an independent basis for expanding Governmental Informational Authority.

#### **(g) Authority-Capability Correspondence**

A Government Agency shall design, procure, configure, and operate its information systems so that Standing Technical Informational Capability corresponds to, and does not materially exceed, Necessary Standing Informational Capability, which 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. Such capability shall otherwise be unavailable through ordinary standing access.

## **Section 7. Fiduciary Duties**

Every Secondary Information Fiduciary owes the following duties with respect to governmental informational activity.

#### **(a) Duty of Loyalty**

A Secondary Information Fiduciary shall exercise informational power faithfully to the lawful governmental relationship, function, and sufficiently particular purpose giving rise to that power. A Secondary Information Fiduciary may not exploit informational possession, access, institutional

position, or technical capability for an unrelated governmental, institutional, political, commercial, or private advantage. The Duty of Loyalty does not prohibit government from undertaking a lawful function merely because the function may be adverse to an individual, including lawful taxation, regulation, investigation, enforcement, adjudication, prosecution, fraud prevention, public health action, child protection, or protection of other persons.

#### **(b) Duty of Care**

A Secondary Information Fiduciary shall exercise reasonable and appropriate care in: (1) determining whether information is necessary for an authorized purpose; (2) minimizing unnecessary informational exposure; (3) maintaining reasonable accuracy, integrity, provenance, and contextual reliability; (4) selecting verification rather than collection where verification reasonably satisfies the governmental need; (5) evaluating the reliability and limitations of material correlations and inferences; (6) securing information and informational systems; (7) correcting, invalidating, superseding, or appropriately qualifying materially inaccurate information or derived informational artifacts; (8) reviewing materially changed systems or informational capabilities; and (9) avoiding Standing Technical Capability materially broader than legitimate governmental need.

#### **(c) Duty of Confidentiality**

A Secondary Information Fiduciary shall protect Individual Information and Relational Information against unauthorized access, acquisition, disclosure, export, correlation, inference, profiling, reuse, commercial exploitation, and governmental exploitation for materially unrelated purposes.

#### **(d) Duty of Transparency and Accountability**

A Secondary Information Fiduciary shall maintain records and controls reasonably sufficient to permit authorized review of material governmental informational acts, including the purpose, authority, actor or system, operation, relevant information domain, disclosure where applicable, and authorization transition where Material Expansion occurred. Nothing in this subsection requires contemporaneous individual disclosure where such disclosure would unlawfully or materially impair a legitimate investigation, enforcement action, security function, protected proceeding, or other lawful governmental purpose. Where direct individual transparency is lawfully restricted, institutional accountability shall be maintained through appropriate audit, oversight, judicial, legislative, inspector-general, or other lawful review.

#### **(e) Structural Performance of Duties**

Where reasonably feasible, material fiduciary limitations shall be implemented through system architecture, authorization controls, purpose-bound access, technical configuration, contractual controls, or other structural means rather than relying principally upon voluntary operator restraint after generalized access has been provided.

## **Section 8. Authorized Informational Acts and Material Expansion**

### **(a-1) Authentication, Technical Authorization, and Legal Authority**

AUTHENTICATE establishes, to the required assurance level, that a person, entity, device, credential holder, or technical actor is the claimed or entitled actor. AUTHORIZE OPERATION is a technical control permitting a specified actor or system to perform a defined operation. Authentication and technical authorization are implementation operations. Neither constitutes Governmental Informational Authority or Materially Renewed Authorization. A system may

technically authorize an operation only within authority independently sufficient for the governmental act.

#### **(a) Informational Acts Separately Governed**

Governmental authority to perform an informational act shall be evaluated according to the nature of the act. Authorization to VERIFY does not automatically authorize READ. Authorization to READ does not automatically authorize CORRELATE. Authorization to CORRELATE does not automatically authorize INFER. Authorization to obtain information does not automatically authorize DISCLOSE, EXPORT, RETAIN, or use for a materially different governmental consequence.

#### **(b) Material Expansion**

A Government Agency shall determine whether a proposed change in informational activity constitutes a Material Expansion. A Material Expansion includes a material broadening of purpose, Authorized Object, information domain, informational operation, correlation, inference, disclosure, duration, retention, governmental consequence, or Standing Technical Capability.

#### **(c) Materially Renewed Authorization Required**

A Government Agency may not undertake a Material Expansion solely because the information is already possessed, technically accessible, commercially available, interoperable, administratively convenient, predictively useful, or broadly authorized at a high level of generality. Material Expansion requires Materially Renewed Authorization that is both legally sufficient and substantively sufficient under this Act for the expanded informational act.

#### **(d) Authorization Transition**

The authorization transition shall be identifiable and reviewable and shall establish, as appropriate: (1) the new or expanded purpose; (2) the independent source of authority; (3) the Authorized Object; (4) the relevant information domains; (5) the authorized informational operations; (6) the necessity and scope of the expansion; (7) the permitted governmental consequence; (8) the duration or expiration of the expanded authority; and (9) applicable accountability requirements.

#### **(e) Authorization Friction**

Information systems shall not permit materially broader governmental individualized knowledge to be obtained through ordinary standing access where the applicable governmental actor lacks authority for that broader knowledge. Material expansion shall require an authorization transition commensurate with the legal significance of the expanded governmental informational power.

#### **(f) No Uniform Authorization Mechanism Required**

Nothing in this Act requires every Materially Renewed Authorization to take the form of a warrant, court order, individual consent, or other single authorization mechanism. The legally required mechanism shall depend upon the applicable Constitution, statute, regulation, judicial doctrine, governmental function, and nature of the informational act.

#### **(g) Emergency Authority**

Where law authorizes emergency informational action, government may expand informational capability to the extent reasonably necessary under that authority. Emergency authority shall be limited by purpose, trigger, scope, actor, permitted operations, duration, audit, and termination and shall not become standing generalized access after the emergency authority expires.

## Section 9. Purpose Particularity and Question Particularity

### (a) Purpose Particularity Required

A governmental informational purpose shall be sufficiently particular to permit an independent reviewer to determine: (1) the governmental function being performed; (2) the legal or fiduciary relationship supporting the function; (3) the source of Governmental Informational Authority; (4) the Authorized Object or class of Authorized Objects; (5) the information reasonably relevant to the purpose; (6) information materially outside the purpose; (7) the informational operations reasonably authorized; (8) the permitted governmental consequence; (9) the endpoint, expiration, or review condition of the purpose; and (10) what additional authority would be required materially to expand the purpose.

### (b) Insufficient Generalized Purposes

The following terms, standing alone, do not establish a sufficiently particular governmental informational purpose: government efficiency; public welfare; public safety; program integrity; fraud prevention; analytics; citizen services; innovation; research; security; administrative convenience; or another comparably generalized formulation. A purpose containing such a term may satisfy this section where the actual governmental function and informational activity are otherwise sufficiently particular.

### (c) Question Particularity

Where government conducts material analytical, statistical, investigative, predictive, exploratory, or machine-assisted processing across multiple persons, Authorized Objects, or information domains, the governmental question shall be sufficiently particular to permit an independent reviewer to determine: (1) the question government is authorized to ask; (2) the information domains reasonably relevant to that question; (3) the computational or informational operations authorized; (4) the classes of outputs authorized; (5) the governmental uses or consequences permitted to follow; and (6) materially different questions, outputs, or uses that remain outside the authorization.

### (d) Unknown Answer Permitted

Question Particularity does not require government to know in advance the identity of every person, transaction, relationship, pattern, anomaly, event, or other object that a lawful inquiry may discover. Uncertainty concerning the answer does not authorize uncertainty concerning the governmental purpose, relevant information domains, permitted operations, or permitted consequences.

### (e) Anti-Abstraction Rule

A Government Agency shall not cure Purpose Divergence by redescribing a governmental purpose at a higher level of abstraction. Terms including government efficiency, public welfare, public safety, citizen services, program integrity, fraud prevention, modernization, research, analytics, innovation, security, data-driven government, and administrative convenience do not, standing alone, establish Legitimate Informational Authority. A purpose using such a term must still identify a sufficiently particular governmental function, relationship or predicate, Authorized Object, question, information domains, authorized operations, necessity, permitted consequence, duration, accountability, and authorization transition.

### (f) Purpose-Divergence and Informational Justification

The justification required for governmental informational power increases as the proposed informational act materially diverges from the Originating Informational Purpose, expands beyond what is necessary to resolve that purpose, crosses purposes or relationships, increases comprehensiveness, creates materially new individualized or relational knowledge, increases governmental consequence, or creates durable or reusable standing capability. The DTA shall implement four Informational Justification Levels: IJ-1, Purpose-Constitutive; IJ-2, Purpose-Protective; IJ-3, Purpose-Divergent; and IJ-4, Purpose-Generalized. IJ-4 standing capability is presumptively prohibited unless a specific enacted provision expressly authorizes and sufficiently bounds the capability.

#### **(e) Purpose Laundering Prohibited**

A Government Agency may not use a generalized governmental objective as a nominal purpose to create Standing Technical Capability materially broader than the authority and function actually supporting the governmental activity.

## **Section 10. Purpose Sequestration, Correlation, Inference, and Authorized Reuse**

#### **(a) Purpose Sequestration**

Government Agencies shall preserve functionally meaningful boundaries among materially distinct governmental informational purposes. Information available for one governmental purpose shall not become ordinarily available for a materially different governmental purpose solely because the same Government Agency possesses it, another Government Agency possesses it, the information exists on shared infrastructure, an application programming interface permits access, a common identifier permits matching, a federated query can retrieve it, an artificial intelligence system can access or infer from it, a contractor or vendor can retrieve it, the information is commercially available, or technical integration makes reuse efficient.

#### **(b) Logical Rather Than Mandatory Physical Separation**

Purpose Sequestration does not require every governmental purpose to operate on physically separate infrastructure. A shared platform, cloud environment, database technology, identity system, or other common infrastructure may comply with this Act where technical and organizational controls preserve the informational boundaries required by law and prevent unauthorized standing cross-purpose capability.

#### **(c) Inherent Processing**

Inherent Processing reasonably necessary to execute an Authorized Informational Act within an existing sufficiently particular purpose does not constitute a separate Material Expansion merely because calculation, comparison, or limited inference occurs.

#### **(d) Material Secondary Correlation**

A Material Secondary Correlation may be performed only where government possesses authority sufficient for the correlation itself and not merely authority to possess or separately access the component information. In determining whether correlation is authorized, the Government Agency shall consider the governmental purpose, information domains involved, Authorized Object, nature and extent of the new individualized or relational knowledge created, applicable

predicates, permitted governmental consequence, duration and retention, and whether Materially Renewed Authorization is required.

#### **(e) Material Derived Inference**

A Material Derived Inference shall be treated as a distinct informational artifact for purposes of this Act. Government shall not create, retain, disseminate, or act materially upon a Material Derived Inference merely because it possesses the underlying information or because a governmental or nongovernmental system is technically capable of producing the inference. Material Derived Inferences shall be subject, as applicable, to sufficient authority; purpose and Question Particularity; provenance; reliability assessment; preservation of epistemic status; correction, invalidation, supersession, or contextual qualification; retention limitations; disclosure limitations; contestability where the inference materially affects an individual; and GAAFA where an Automated Decision System or artificial intelligence system is involved.

#### **(f) Epistemic Status**

A prediction, anomaly, risk signal, association, correlation, classification, or inference shall not be treated as an established fact merely because it has been generated, stored, or displayed by a governmental system. Government shall preserve the distinction among analytical signal, validated information, verified finding, and adjudicative fact.

#### **(g) Authorized Reuse**

Information lawfully obtained for one purpose may be reused for a materially different governmental purpose only where: (1) the recipient governmental function possesses independently sufficient authority; (2) the recipient purpose is sufficiently particular; (3) the reuse is necessary and appropriately bounded; (4) the informational operations to be performed are authorized; (5) any Material Expansion receives Materially Renewed Authorization; (6) retention and redisclosure are appropriately bounded; (7) provenance and accountability are preserved; and (8) the reuse does not functionally merge the source and recipient informational domains into standing generalized access.

#### **(h) Reuse Does Not Merge Domains**

An Authorized Reuse transaction does not convert separate governmental informational domains into a common governmental information pool and does not establish continuing authority for subsequent cross-purpose access.

#### **(i) Interoperability Without Integration**

Nothing in this section prohibits lawful interoperability among governmental systems. Interoperability shall be structured so that each material cross-purpose informational transaction remains attributable to a lawful purpose, sufficient authority, defined informational act, and accountable governmental function.

#### **(j) Verification and Minimum Knowledge Exposure**

Where a governmental purpose can reasonably be satisfied by verification of a fact, status, eligibility condition, or other bounded proposition without acquisition of materially broader underlying information, the Secondary Information Fiduciary shall prefer the less informationally expansive method unless law requires acquisition or retention of the underlying information, the underlying information is reasonably necessary for adjudication, evidence, contestability, audit, or due process, verification alone is materially inadequate to perform the authorized

governmental function, or another legally sufficient reason requires the broader informational act.

#### **(k) Construction**

This section shall be construed to permit government to perform legitimate cross-domain functions while preventing Standing Technical Capability for generalized governmental informational power. A legitimate use case does not independently justify an architecture that leaves materially broader informational capability available through ordinary standing access after the use case has ended.

## **Section 11. Bounded Government Discovery and Progressive Particularization**

#### **(a) General Rule**

A Government Agency may conduct discovery, investigation, analysis, comparison, or other informational activity without knowing in advance the identity of every person or other Authorized Object that may be discovered, provided that the activity constitutes Bounded Government Discovery under this section. The absence of a known answer does not create generalized authority over the information used to seek that answer.

#### **(b) Bounded Government Discovery**

"Bounded Government Discovery" means governmental informational activity undertaken pursuant to independently sufficient authority in which: (1) the governmental purpose is sufficiently particular under Section 9; (2) the Government Agency has identified the Authorized Object, class of Authorized Objects, event, transaction, relationship, pattern, risk, condition, or other lawful object of inquiry at the level of particularity reasonably available at that stage; (3) the information domains subject to discovery are defined and reasonably related to the governmental purpose; (4) the informational and computational operations that may be performed are defined or otherwise lawfully bounded; (5) the permitted outputs are defined or bounded; (6) the governmental consequences that may follow from an output are defined or bounded; (7) applicable predicates, authorization transitions, retention limitations, and accountability requirements are established; and (8) the discovery does not create Standing Technical Capability to formulate materially unconstrained individualized questions across materially unrelated information domains.

#### **(c) Forms of Bounded Government Discovery**

(1) Predicate-Bounded Discovery. Discovery directed by an objective factual, legal, investigative, programmatic, or other lawful predicate that defines the object, scope, domain, or condition being investigated.

(2) Hypothesis-Generating Analytics. Exploratory analysis designed to identify previously unknown patterns, anomalies, relationships, transactions, or other signals may be conducted without a preidentified individual where: (A) the governmental mission is lawful and sufficiently particular; (B) the information domains are defined; (C) the analytical operations are authorized or bounded; (D) the permitted output is limited to a signal, hypothesis, pattern, or other appropriately qualified analytical result; (E) the output does not by itself constitute an adjudicative fact or sufficient basis for a materially adverse governmental action; (F) individualized investigation or materially expanded use requires the authorization transition

required by subsection (f); and (G) the activity otherwise satisfies this Act and GAAFA where applicable.

(3) Statistical Discovery. Government may perform statistical or population-level analysis where the resulting information satisfies the requirements applicable to Statistical Information and the activity does not create unauthorized individualized or relational governmental knowledge.

#### **(d) Generalized Discovery Prohibited**

A Secondary Information Fiduciary may not conduct or maintain capability for materially generalized discovery consisting of substantially unconstrained authority to search materially unrelated governmental or nongovernmental information domains; identify persons, relationships, transactions, activities, or patterns for unspecified governmental purposes; formulate materially unconstrained individualized questions after access has been granted; use discovered information for materially different governmental purposes without Materially Renewed Authorization; or retain generalized discovery capability as ordinary Standing Technical Capability merely because the capability may occasionally support a legitimate governmental function.

#### **(e) Objective Predicate**

Where this Act, another applicable law, a judicial authorization, or the governing legal standard requires a predicate before individualized discovery, correlation, identification, or investigation, the predicate shall be: (1) articulable; (2) objectively reviewable; (3) materially related to the governmental purpose; (4) sufficient under the law governing the informational act; and (5) recorded in a manner adequate for subsequent accountability, except where law expressly provides otherwise. A Government Agency may also impose an Objective Predicate as an architectural safeguard where not independently required by law. No such internally imposed predicate enlarges Governmental Informational Authority. A conclusory label, generalized suspicion, administrative preference, or unsupported characterization of a person as a "person of interest," "risk," "threat," or similar designation does not independently satisfy this subsection.

#### **(f) Progressive Particularization**

Where Bounded Government Discovery produces information that identifies or materially particularizes a person, relationship, transaction, event, location, device, organization, or other Authorized Object, the Government Agency shall determine whether further informational activity would constitute a Material Expansion. Where Material Expansion would occur, the Government Agency shall obtain Materially Renewed Authorization before exercising the expanded informational capability.

*AUTHORIZED DISCOVERY → SIGNAL → VALIDATION → PARTICULARIZATION EVENT → MATERIALLY RENEWED AUTHORIZATION → INVESTIGATION, REVIEW, OR OTHER AUTHORIZED ACTION.*

#### **(g) Analytical Signals**

An anomaly, association, prediction, risk score, statistical result, machine-generated signal, or other analytical output produced through Bounded Government Discovery shall retain its appropriate epistemic status; does not by itself establish misconduct, liability, ineligibility, fraud, criminal activity, or another adjudicative fact; shall not independently support a materially adverse governmental action unless applicable law permits such action on that evidentiary basis;

and shall be subject to GAAFA where produced or materially evaluated by an Automated Decision System or artificial intelligence system.

#### **(h) Population Scale**

Processing a large population or number of records does not by itself render an informational activity generalized or nonconforming. The relevant inquiry is whether the governmental question, information domains, operations, outputs, permitted consequences, and authorization transitions remain sufficiently bounded.

#### **(i) Retrospective Discovery**

The fact that information was lawfully collected or retained before a governmental inquiry arose does not independently authorize retrospective search, correlation, inference, or reconstruction. Retrospective discovery shall satisfy the same requirements of purpose, authority, particularity, operation, and permitted consequence applicable to contemporaneous discovery.

#### **(j) Federated and Intergovernmental Discovery**

A federated search, shared investigative platform, fusion environment, task force, or intergovernmental information system shall not aggregate the separate informational authorities of participating governmental entities into a collective general authority. Each material informational act shall be supported by authority sufficient for the governmental actor, purpose, and operation involved.

## **Section 12. Independent Information Intermediation**

#### **(a) Purpose**

This section governs governmental informational relationships with private or nongovernmental entities that independently aggregate, enrich, correlate, profile, infer from, license, sell, disclose, or otherwise exercise material informational capability concerning persons. This section shall be construed to prevent government from enlarging its informational authority through private informational intermediaries while permitting bounded commercial services reasonably necessary to legitimate governmental functions.

#### **(b) Independent Information Intermediary**

"Independent Information Intermediary" or "III" means a nongovernmental person or entity that, independently of the bounded governmental transaction at issue, possesses or exercises material capability to acquire individualized information from multiple sources; aggregate or enrich individualized information; resolve identities across sources or contexts; construct behavioral, relational, commercial, location, biometric, or other individualized profiles; correlate information across contexts; generate individualized scores, classifications, predictions, relationships, or inferences; license, sell, redisclose, or otherwise commercially distribute individualized information or informational products; or reuse individualized information for a purpose materially independent of the governmental transaction. Classification depends upon functional informational capability and conduct, not the entity's corporate designation or characterization of itself.

### **(c) Bounded Processor Distinguished**

A contractor, vendor, or service provider is not an Independent Information Intermediary with respect to a particular governmental transaction solely because it processes information on behalf of government where the entity: (1) acts only pursuant to bounded governmental instructions; (2) lacks independent authority to use the information for its own purposes; (3) may not materially combine the information with unrelated information; (4) may not sell, license, redisclose, enrich, profile, or independently infer from the information; (5) is subject to defined retention and deletion or return obligations; (6) is subject to audit and enforceable contractual or legal restrictions; and (7) does not maintain generalized informational capability for government through another contractual or technical arrangement. The substance of the relationship controls over contractual labels.

### **(d) Presumption of Disloyal 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 Duty of Loyalty where the transaction exposes individualized information to independent aggregation, enrichment, profiling, sale, redisclosure, unrelated reuse, or model training; or provides government materially broader individualized knowledge or informational capability than the authority supporting the governmental purpose. The presumption may be rebutted only as provided by this section and Section 13.

### **(e) Government-to-Intermediary Disclosure**

A Secondary Information Fiduciary may disclose Individual Information or Relational Information to an Independent Information Intermediary only upon a showing sufficient under Section 20 that: (1) the disclosure is supported by independently sufficient authority; (2) the governmental purpose is sufficiently particular; (3) the disclosure is reasonably necessary to the governmental function; (4) the information disclosed is minimized to that purpose; (5) the intermediary is prohibited from materially unrelated aggregation, enrichment, profiling, sale, licensing, redisclosure, model training, model improvement, product development, or reuse; (6) subcontractors and downstream recipients are subject to equivalent restrictions; (7) retention is bounded; (8) derivative information and informational products are governed; (9) audit and enforcement rights are sufficient; (10) deletion, return, or continued preservation is governed at termination; and (11) the arrangement does not enable government later to reacquire materially expanded information or informational capability without independently sufficient authority. Government-purpose model training, configuration, testing, or improvement may occur where it is reasonably necessary to the authorized governmental function; occurs within the bounded governmental processing relationship; does not permit independent commercial or unrelated use; does not enlarge the intermediary's independent informational capability beyond what is reasonably necessary to perform the governmental function; is subject to applicable retention, deletion, provenance, audit, and security requirements; and complies with GAAFA where applicable.

### **(f) Intermediary-to-Government Acquisition**

A Government Agency may acquire individualized information, an informational product, a correlation, inference, profile, identity-resolution result, score, prediction, or other informational capability from an Independent Information Intermediary only where: (1) the Government Agency

possesses independently sufficient authority to acquire or obtain the informational substance involved; (2) the governmental purpose satisfies Purpose Particularity; (3) Question Particularity is satisfied where the acquisition supports analytical, predictive, investigative, or exploratory processing; (4) the acquisition is reasonably necessary and appropriately bounded; (5) the information domains and scope are defined; (6) government possesses authority for the informational operations embodied in or to be performed upon the acquired information; (7) the permitted governmental consequence is defined; (8) material provenance sufficient to evaluate the information or product is available; (9) applicable retention, correction, contestability, and disclosure rules are satisfied; and (10) the acquisition does not circumvent a legal, constitutional, fiduciary, architectural, or procedural limitation that would apply if government obtained or constructed the informational substance directly.

#### **(g) Commercial Availability Does Not Create Authority**

The lawful possession, publication, licensing, sale, accessibility, or commercial availability of information by an Independent Information Intermediary does not independently establish governmental authority to acquire, query, correlate, infer from, retain, or act upon that information.

#### **(h) Informational Transformation Does Not Cure Lack of Authority**

A governmental informational act does not become authorized merely because a nongovernmental person has aggregated underlying information; correlated information across sources; resolved identities; transformed information; generated a score or classification; produced a prediction; inferred an attribute or relationship; or otherwise converted underlying information into a different informational product. Government may not outsource an informational act it lacks authority to perform and acquire the informational result as a substitute for that authority.

#### **(i) Government Reacquisition Loop**

Where information originating with government is disclosed or made available to an Independent Information Intermediary; aggregated, enriched, correlated, modeled, profiled, transformed, or combined with other information; and subsequently acquired, queried, licensed, or otherwise made available to government, the disclosure and reacquisition shall be evaluated as a single composite informational relationship where functionally related. A Government Agency may not establish or participate in a standing Government-Intermediary Reacquisition Architecture that functionally creates generalized individualized governmental knowledge beyond the Government Agency's standing authority.

#### **(j) Architectural Substitution Test**

A Government Agency shall evaluate whether an intermediary relationship creates substantially the same governmental or intermediary informational capability that would violate this Act if constructed directly within government. The use of an intermediary does not cure an otherwise prohibited informational architecture.

#### **(k) Commercial Surveillance Information**

Nothing in this section precludes the Legislature from imposing a warrant, court-order, subpoena, statutory prohibition, or other heightened acquisition standard upon defined categories of commercially compiled surveillance information. Where another provision of law imposes a more protective acquisition standard, the more protective standard governs.

### **(I) Verification Alternative**

Where a legitimate governmental purpose can be satisfied through a bounded verification transaction with an Independent Information Intermediary without government acquiring materially broader underlying information, the Government Agency shall prefer the less informationally expansive transaction where reasonably practicable and legally sufficient.

## **Section 13. Presumptively Disloyal Practices**

### **(a) Presumption**

The practices described in this section are presumptively inconsistent with the fiduciary duties established by Section 7. The presumption places upon the Secondary Information Fiduciary the burden established by Section 20 to demonstrate that the challenged informational act was supported by sufficient authority, sufficiently particular purpose, necessity, appropriately bounded scope, authorized informational operations, permitted consequence, and other requirements applicable under this Act. Individual consent alone does not rebut a presumption where the informational act requires independent governmental authority or where the conduct materially exceeds the scope of the consent.

### **(b) Presumptively Disloyal Practices**

It is presumptively disloyal for a Secondary Information Fiduciary to: (1) use, process, query, or disclose Individual Information or Relational Information for a purpose materially different from the purpose supporting the information's acquisition or prior use without independently sufficient authority and, where required, Materially Renewed Authorization; (2) perform Material Secondary Correlation across unrelated or materially distinct governmental, commercial, institutional, or transactional contexts; (3) create, retain, disclose, or materially act upon a Material Derived Inference without satisfying Sections 8 through 10 and GAAFA where applicable; (4) identify, re-identify, resolve the identity of, or associate previously unidentified or pseudonymous information with a natural person where the identification materially expands governmental individualized knowledge; (5) disclose Individual Information or Relational Information to a nongovernmental person for a purpose not reasonably necessary to the governmental function or without sufficient legal and fiduciary safeguards; (6) enter into a government-to-intermediary disclosure, intermediary-to-government acquisition, or comparable relationship described in Section 12; (7) obtain or request information materially beyond what is reasonably necessary and authorized for the governmental purpose; (8) retain information beyond the period supported by active processing authority, lawful preservation authority, records law, adjudicative necessity, audit requirements, or another independently sufficient legal basis; (9) permit an employee, official, administrator, contractor, agent, automated system, or other actor to exercise informational capability for a purpose materially outside that actor's authorized governmental function; (10) characterize a generalized objective, including "public safety," "program integrity," "fraud prevention," "analytics," "efficiency," "citizen services," "security," or similar language, as sufficient authority for informational activity that does not satisfy Section 9; (11) use administrator, superuser, debugging, recovery, security, maintenance, or other technical privilege to perform a substantive governmental informational act not otherwise authorized; (12) obtain or use information through another Government Agency, political subdivision, sovereign, fusion environment, task force, or governmental partner where the receiving governmental function lacks independently sufficient authority for the informational act; (13) acquire materially

broader underlying information where a less informationally expansive verification method is reasonably practicable and lawfully satisfies the governmental need, absent a sufficient justification under Section 10(j); (14) maintain Individual Information, Relational Information, derived information, or material informational capability without safeguards reasonably commensurate with the sensitivity, consequence, and capability involved; (15) fail to maintain records reasonably sufficient to permit authorized review of material informational acts, subject to lawful restrictions on disclosure; (16) refuse without sufficient legal basis to correct, invalidate, supersede, or appropriately qualify materially inaccurate Individual Information or a materially inaccurate derived informational artifact where the Secondary Information Fiduciary possesses authority and practical ability to do so; or (17) search, correlate, reconstruct, or analyze historically retained information to create materially new individualized knowledge concerning past conduct without sufficient authority for the retrospective informational act.

### **(c) Rebuttal**

A Secondary Information Fiduciary rebuts a presumption under this section only by establishing, by the evidentiary standard provided in Section 20, as applicable: (1) a sufficiently particular governmental purpose; (2) independently sufficient authority; (3) necessity or legally appropriate relationship between the informational act and governmental function; (4) an appropriate Authorized Object or lawful discovery scope; (5) authorized information domains; (6) authority for the informational operation performed; (7) compliance with applicable predicate requirements; (8) appropriate minimization; (9) a defined permitted consequence; (10) appropriate duration, retention, and disclosure limitations; (11) Materially Renewed Authorization where Material Expansion occurred; and (12) compliance with applicable fiduciary and architectural safeguards.

### **(d) No Rebuttal by Convenience**

The presumption may not be rebutted solely by administrative convenience, cost savings, technical capability, predictive usefulness, interoperability, possession of the information, commercial availability, generalized service improvement, a vendor's ordinary business practices, or generalized consent unrelated to the challenged informational act.

### **(e) Relationship to Section 14**

Conduct classified as per se disloyal under Section 14 is not governed by the rebuttable presumption established by this section.

## **Section 14. Per Se Disloyal Practices**

### **(a) General Rule**

The practices described in this section are incompatible with the fiduciary relationship established by this Act and constitute per se breaches of the Duty of Loyalty. Except where a subsection expressly provides otherwise, a practice classified as per se disloyal is not rendered lawful by individual consent, terms of service, administrative convenience, cost savings, technical capability, commercial availability, predictive usefulness, interagency agreement, vendor contract, or generalized governmental interest. A constitutionally sufficient warrant, court order, subpoena, or other judicial authorization may authorize a particular informational act to the extent provided by applicable law. Judicial authorization of a particular informational act does not by itself authorize construction or maintenance of Standing Technical Capability prohibited

by this section. A prohibited structural capability may be authorized only where enacted law expressly authorizes that capability, sufficiently defines its governmental purpose and scope, and the capability otherwise satisfies applicable constitutional requirements.

#### **(b) Per Se Disloyal Practices**

It is per se disloyal to: (1) construct, procure, maintain, or operate Standing Technical Capability whose ordinary designed function permits governmental actors to construct materially comprehensive cross-purpose individualized knowledge concerning persons without Materially Renewed and sufficiently particular authorization; (2) construct, maintain, procure, or operate a Government Population Golden Record; (3) provide a Governmental Actor with Functional Universal Search; (4) create or maintain materially generalized technical access and rely principally upon policy, training, contractual language, user promises, or after-the-fact auditing to prevent governmental actors from exercising informational capability that they lack standing authority to exercise; (5) maintain administrative, superuser, maintenance, recovery, security, vendor, or equivalent access that permits ordinary substantive cross-purpose governmental use without independently controlled authorization appropriate to the exceptional privilege; (6) use a vendor, contractor, Independent Information Intermediary, artificial intelligence system, shared service, governmental partner, another sovereign, or another governmental component to obtain or exercise materially generalized informational capability that the governmental function could not lawfully maintain or exercise directly; (7) establish or maintain a standing Government-Intermediary Reacquisition Architecture; (8) knowingly designate a materially generalized or fictitious purpose for the purpose of avoiding particularity, authorization, warrant, consent, minimization, or other substantive requirements that would apply to the actual governmental informational activity; (9) knowingly design or operate a system so that a Governmental Actor or automated system may materially expand individualized governmental knowledge through ordinary standing access without an authorization transition required by Section 8; (10) design or operate an intergovernmental information arrangement on the premise that the separate authorities of participating governmental entities collectively create generalized authority available to each participant, where no participant independently possesses sufficient authority for the informational act performed; (11) direct, procure, induce, or knowingly rely upon a third party or automated system to aggregate, correlate, identify, infer, score, profile, or otherwise transform information for the purpose of acquiring an informational result that government lacks authority to construct or obtain directly; (12) sell, license, monetize, commercially profile, or use for materially unrelated commercial advantage Individual Information or Relational Information obtained or held through a governmental fiduciary relationship, except where expressly required by law and consistent with the fiduciary purpose; (13) use information obtained through one governmental relationship, credential presentation, service request, benefit interaction, or other informational context as the basis for retaliation, discrimination, exclusion, punishment, or materially adverse governmental treatment in a materially unrelated context where government lacks independently sufficient authority for that use; or (14) knowingly destroy, materially falsify, conceal, or cause the omission of an audit record, authorization record, provenance record, material system capability, or material informational transaction for the purpose of preventing review or enforcement under this Act; or (15) construct, procure, maintain, or operate ordinary Standing Technical Informational Capability that materially exceeds Necessary Standing Informational Capability, even where the broader capability lies within an outer boundary of Standing Legitimate Informational Authority, unless the broader capability is unavailable through

ordinary standing access and activates only upon the predicate, authorization transition, and necessity required for the resulting legitimate function.

**(c) Cross-Context Correlation Not Per Se by Itself**

Material Secondary Correlation is not a per se violation merely because information from more than one context or domain is correlated. Correlation is governed by Sections 8 through 13 and becomes per se disloyal where it is performed through or forms part of a practice prohibited by subsection (b).

**(d) Reverse Identification Not Per Se by Itself**

Identification, re-identification, or identity resolution is not a per se violation merely because the person did not actively present a credential in the transaction. Such activity is governed by Sections 8 through 13 and applicable constitutional or statutory predicates. This subsection shall not be construed to authorize generalized standing identity resolution.

**(e) Legitimate Surveillance and Investigation Distinguished**

The term "surveillance," standing alone, does not determine whether conduct violates this section. Lawfully authorized observation, investigation, monitoring, discovery, audit, security activity, or enforcement may be permissible where bounded by sufficient authority, particularity, applicable predicates, authorized operations, duration, and accountability. Standing generalized informational surveillance prohibited by subsection (b)(1) remains per se disloyal.

**(f) Individual Consent Does Not Cure Structural Excess**

An individual's consent does not cure a system architecture that creates generalized governmental informational capability materially exceeding the authority of the governmental function.

**(g) Applicability to Automated Systems and Agents**

A Government Agency remains responsible under this section where a prohibited practice is performed by an artificial intelligence system, automated agent, contractor, vendor, or other system acting within capability made available for the governmental function. Autonomous initiation by the system does not alter the classification of the informational act.

**(h) Vendor Consequences**

A Vendor's violation of an express Vendor duty, contractual conformance obligation, procurement requirement, or knowing or reckless participation in a prohibited governmental capability constitutes grounds, as authorized by law, for suspension of the affected capability, contract remedies, termination for cause, remediation, debarment, and other applicable relief. This subsection does not convert the Vendor into a governmental fiduciary.

**(i) Government Consequences**

A per se violation by a Government Agency is enforceable under Sections 21 through 23 and is subject to structural remedies sufficient to remove or materially constrain the prohibited capability.

## **Section 15. Rights of Primary Information Trustees**

### **(a) General Rule**

A Primary Information Trustee has the rights established by this section with respect to Individual Information concerning that person that is obtained, possessed, processed, generated, correlated, inferred from, disclosed, retained, or otherwise subject to Governmental Informational Power. The rights established by this section are cumulative; may not be waived through a contract, terms of service, privacy policy, adhesion agreement, or similar instrument; do not depend upon ownership of the underlying information; do not extinguish independently sufficient governmental authority; shall be implemented consistently with lawful investigative, adjudicative, preservation, public-record, security, and other governmental obligations; and shall be enforceable as provided by this Act.

### **(b) Right to Know**

A Primary Information Trustee has the right, upon a verified request and subject to subsection (n), to know whether a Government Agency possesses or exercises material informational capability concerning that individual. The response shall identify, to the extent reasonably available and lawfully disclosable: categories of Individual Information held or materially accessible; governmental purposes; sources; legal authority; material information domains; material disclosures; retention or preservation periods; whether Material Secondary Correlation or Material Derived Inference materially affected the individual's record, status, eligibility, rights, obligations, or governmental treatment; whether an Independent Information Intermediary materially supplied information or capability; and means of exercising rights under this section.

### **(c) Right of Access**

A Primary Information Trustee has the right to obtain, in a reasonably intelligible form: Individual Information concerning that person maintained by a Government Agency; material derived informational artifacts retained or materially relied upon; material provenance reasonably necessary to understand the origin and status of such information; material records of disclosure; material records of access or processing where disclosure is required under this Act or implementing standards; and information necessary to understand how to seek correction, contest an inference, challenge an adverse governmental action, or pursue a remedy. Access shall be provided without requiring the individual to surrender additional information materially beyond what is reasonably necessary to authenticate the request.

### **(d) Right to Purpose and Authority Disclosure**

Where government undertakes a material individualized informational act concerning a Primary Information Trustee, the individual has the right, subject to subsection (n), to obtain a reasonably intelligible statement of the governmental purpose; whether the purpose is Citizen-Originated or Authority-Originated; the source of Governmental Informational Authority; the material informational operations performed; any Materially Renewed Authorization materially affecting the individual's information; and the governmental consequence for which the information was or may be used. Nothing in this subsection requires disclosure of information protected by law, privileged material, investigative methods lawfully withheld, or information whose disclosure would materially impair an authorized governmental function.

#### **(e) Right to Notice**

A Primary Information Trustee has the right to reasonable notice of material governmental informational activity concerning that person as provided by this subsection. (1) Citizen-Originated Purpose. For a Citizen-Originated Purpose, the Government Agency shall provide notice at or before the point reasonably appropriate to the interaction describing the governmental purpose; categories of information reasonably sought; material informational operations reasonably anticipated; material disclosures reasonably anticipated; whether individual authorization is requested and whether the requested authorization is optional or required for the requested governmental function; material retention practices; and means of exercising rights under this Act. (2) Authority-Originated Purpose. For an Authority-Originated Purpose, notice shall be provided when required by applicable law or when reasonably practicable without materially impairing the lawful governmental function. (3) Delayed Notice. Notice may be delayed where contemporaneous notice would materially impair an authorized investigation, enforcement, fraud detection, protection of a person, system or cybersecurity, an authorized confidential proceeding, or another governmental function for which delayed notice is authorized by law. Where the basis for delayed notice expires, notice shall be provided when required by applicable law or this Act unless an independently sufficient basis for continued nondisclosure exists. (4) No Notice as Authority. Providing notice does not itself establish Governmental Informational Authority. Failure to object to notice does not constitute consent.

#### **(f) Right to Correction**

A Primary Information Trustee may request correction of materially inaccurate, incomplete, misleading, misattributed, or materially decontextualized Individual Information maintained by a Government Agency. Upon a verified request, the Government Agency shall, within [30] days or another period established by rule, correct the information; deny the request in whole or in part and provide the factual and legal basis for denial; indicate that the information is disputed where immediate correction cannot reasonably be completed; notify materially affected downstream governmental recipients where correction is required and reasonably practicable; and preserve any prior version where required for audit, evidence, public records, adjudication, legal hold, or another lawful preservation purpose while preventing the superseded information from being presented as current fact.

#### **(g) Right to Correction of Derived Information**

Where a Material Derived Inference, score, classification, relationship, prediction, or analytical signal concerning a Primary Information Trustee is materially inaccurate, obsolete, unsupported, or based upon materially inaccurate source information, the individual may request correction, invalidation, supersession, contextual qualification, or notation of dispute. A Government Agency may not deny relief solely on the ground that the challenged information is an inference, prediction, model output, or analytical product rather than a directly observed fact.

#### **(h) Right to Revocation of Individual Authorization**

Where Governmental Informational Authority depends solely upon authorization provided by the Primary Information Trustee, the individual may revoke that authorization prospectively. The Government Agency shall give effect to revocation within a reasonable period not to exceed [72 hours], unless applicable law requires a different period; independently sufficient governmental authority supports continued processing; lawful preservation obligations require retention; completion of an existing adjudicative, enforcement, audit, or records process requires

continued limited processing; or immediate cessation is technically impracticable and temporary continuation is narrowly necessary to implement revocation safely. The Government Agency bears the burden of identifying any independent authority relied upon after revocation.

#### **(i) No General Veto Over Independent Governmental Authority**

Nothing in this Act creates an individual veto over informational activity independently authorized by law. A Primary Information Trustee nevertheless retains all rights under this Act to challenge whether the claimed authority exists; whether the purpose is sufficiently particular; whether the information or informational operation is necessary and within scope; whether Material Expansion occurred without Materially Renewed Authorization; whether fiduciary duties were breached; and whether the resulting governmental consequence was lawful.

#### **(j) Right to Deletion or Termination of Active Use**

A Primary Information Trustee may request deletion of Individual Information or termination of its active governmental use where the authority supporting active processing has expired; the information is no longer reasonably necessary for an authorized purpose; the information was obtained or retained unlawfully; individual authorization upon which processing solely depended has been revoked; or another provision of law requires deletion. Where deletion is prohibited or inappropriate because lawful preservation authority remains, the Government Agency shall cease unauthorized active processing and place the information under controls appropriate to preservation-only status.

#### **(k) Right to Portability**

A Primary Information Trustee has the right, where technically feasible and not prohibited by law, to receive Individual Information maintained by government concerning that person in a structured, commonly used, machine-readable, and interoperable format. Portability shall preserve provenance reasonably necessary to understand the information; distinguish governmental assertions from individual assertions and derived information where material; not require transfer to a particular commercial platform or provider; support movement among lawful and standards-compliant tools where applicable; and be implemented consistently with VIDA.

#### **(l) Right to Delegation**

A Primary Information Trustee may delegate specified rights under this Act to an Authorized Information Trustee in accordance with Section 16. Delegation does not transfer or extinguish Primary Information Trusteeship.

#### **(m) Right to Explanation and Contestability**

Where a governmental decision materially affecting a right, benefit, service, license, obligation, status, liberty interest, or comparable interest is based materially upon a Material Derived Inference, an Automated Decision System, artificial intelligence, a material risk score or classification, or a materially disputed informational artifact, the Primary Information Trustee shall have a right to explanation, contestability, and review as provided by this Act, applicable due process law, and GAAFA.

#### **(n) Lawful Limitations on Disclosure**

A Government Agency may delay, limit, or deny disclosure otherwise required under subsections (b) through (d) only to the extent reasonably necessary and authorized by law to protect an active criminal, civil, regulatory, or administrative investigation; confidential investigative

methods or sources; another person's legally protected information; attorney-client privilege, attorney work product, deliberative privilege where recognized, or another lawful privilege; national security or protected intelligence information; cybersecurity or system security where disclosure would create a material risk; child-protection or comparable protected proceedings; or another interest expressly protected by law. Any limitation shall be no broader or longer than reasonably necessary. Where practicable and lawful, the Government Agency shall provide segregable information not subject to restriction, the legal basis for withholding, a general description of the withheld category, and a means of administrative or judicial review.

#### **(o) No Rights Penalty for Individual Error**

A Primary Information Trustee shall use reasonable efforts not knowingly to submit materially false information to government. An individual's failure to maintain perfect accuracy, however, does not diminish the individual's rights under this Act or relieve a Secondary Information Fiduciary of its duties.

## **Section 16. Authorized Information Trustees and Guardianship**

#### **(a) Authority to Delegate**

A Primary Information Trustee may designate an Authorized Information Trustee to exercise specified informational rights or responsibilities on the individual's behalf. A designation shall identify, as applicable, the principal; the Authorized Information Trustee; information domains covered; permitted purposes; permitted informational acts; duration; authority to delegate, if any; revocation conditions; and accountability requirements.

#### **(b) Forms of Authorized Information Trusteeship**

An Authorized Information Trustee may include: (1) a designated representative; (2) an attorney or legal representative; (3) a parent; (4) a court-appointed guardian; (5) a conservator or comparable fiduciary; (6) a health, financial, benefits, disability, or professional representative acting within lawful authority; (7) an institutional fiduciary expressly authorized to act on behalf of the Primary Information Trustee; (8) a natural person or legally cognizable entity using a technical agent or artificial intelligence assistant to exercise delegated informational authority, where permitted by law; or (9) another natural person or legally cognizable fiduciary authorized by law.

#### **(c) Duties of an Authorized Information Trustee**

An Authorized Information Trustee shall act within the scope of the authorization; exercise delegated informational authority faithfully to the interests and lawful directions of the Primary Information Trustee; exercise reasonable care; maintain confidentiality; avoid unauthorized aggregation, correlation, disclosure, or reuse; maintain accountability appropriate to the delegated authority; and avoid using informational possession for the trustee's materially unrelated advantage.

#### **(d) No Transfer of Primary Trusteeship**

Designation of an Authorized Information Trustee does not transfer Primary Information Trusteeship. Possession of credentials, records, keys, wallet access, delegated authority, or technical control does not make the Authorized Information Trustee the Primary Information Trustee.

#### **(e) Anti-Recentralization**

An Authorized Information Trustee, wallet provider, guardianship platform, credential manager, agent, or institutional fiduciary shall not use delegated informational authority to create materially generalized cross-context informational capability concerning the Primary Information Trustee beyond what is reasonably necessary to perform the delegated function. Government may not require use of an Authorized Information Trustee arrangement that functionally recreates a Government Population Golden Record or materially expands governmental Standing Technical Capability.

#### **(f) Parent and Guardian Authority**

For a minor, incapacitated person, or other person legally unable to exercise one or more rights under this Act, a parent, guardian, or other legally authorized representative may act as an Authorized Information Trustee to the extent permitted by law. Such authority shall remain bounded to the legal relationship giving rise to it; be exercised with due regard for the represented person's interests, dignity, autonomy, and developmental or decisional capacity; minimize unnecessary informational exposure; terminate or narrow when the legal basis terminates or narrows; and be subject to applicable judicial or administrative oversight.

#### **(g) Restoration of Personal Authority**

Upon reaching majority, restoration of legal capacity, termination of guardianship, or other cessation of substitute authority, the Primary Information Trustee shall regain direct exercise of rights under this Act to the maximum extent provided by law. Government systems shall provide a practical mechanism for transfer, revocation, or reconfiguration of delegated informational authority.

#### **(h) Revocation**

A Primary Information Trustee may revoke a voluntary delegation at any time unless another law independently provides otherwise. Revocation shall terminate prospective authority of the Authorized Information Trustee after a reasonable implementation period.

#### **(i) Government Not Default Authorized Information Trustee**

The inability, unwillingness, or failure of an individual personally to administer credentials, records, or informational rights does not by itself authorize a Government Agency to assume the role of Authorized Information Trustee or to consolidate the individual's information on that basis.

#### **(j) Technical Agents**

An artificial intelligence system, software agent, wallet, credential manager, or other technical system may exercise informational capability on behalf of a Primary Information Trustee or Authorized Information Trustee but does not thereby become the legal trustee unless applicable law independently recognizes the system as a legal person capable of assuming such duties. The natural person or legally cognizable entity deploying or controlling the technical agent remains accountable according to the legal relationship governing its use.

## Section 17. Government, Vendor, Agent, and Intergovernmental Responsibility

### (a) Government Remains Responsible

A Government Agency remains responsible for compliance with this Act when Governmental Informational Power is exercised through employees, contractors, vendors, subcontractors, shared-service providers, cloud providers, artificial intelligence systems, automated agents, Independent Information Intermediaries, another Government Agency, another political subdivision or sovereign, or another person acting on behalf of or materially supporting the governmental function. Delegation of performance does not delegate away governmental fiduciary responsibility.

### (b) Vendor and Contractor Legal and Contractual Obligations

A Vendor, contractor, subcontractor, or agent does not become a Secondary Information Fiduciary merely by contracting with government or exercising technical capability on its behalf. Such person shall possess no greater informational authority or operational permission than the Government Agency may lawfully and legitimately confer for the governmental function involved and is subject to duties expressly imposed by this Act or other law, procurement requirements, contractual covenants, and agency principles where applicable.

#### (b-1) Vendor Liability and Nondelegation

(1) A Vendor is directly subject to a duty under this Act only where the Act expressly imposes that duty upon the Vendor or upon a statutory role the Vendor actually occupies. Vendor status alone does not create governmental fiduciary status.

(2) A Vendor is directly liable for violation of a duty that PDTA, VIDA, or GAAFA expressly imposes upon the Vendor or upon a statutory role occupied by the Vendor.

(3) A Vendor that is not otherwise directly subject to the violated duty may be liable where, with actual knowledge or reckless disregard of the material facts establishing the violation, the Vendor materially causes, directs, or participates in the prohibited informational act or maintains a specifically configured prohibited capability within the Vendor's control after a legally sufficient duty to remediate has arisen.

(4) Mere manufacture, sale, licensing, hosting, or provision of a general-purpose product or service, without conduct described in paragraphs (1) through (3), does not by itself create liability under the trilogy.

(5) A Government Agency's duties under the trilogy are nondelegable. Vendor fault, contractual allocation, or technical operation does not relieve the Government Agency of a duty imposed upon it.

(6) Contractual indemnification may allocate financial responsibility between government and a Vendor only to the extent permitted by law and shall not waive, diminish, or transfer an individual's statutory rights or the DTA's enforcement authority.

### (c) Required Contractual Terms

A governmental contract involving material Individual Information, Relational Information, informational capability, identity services, analytics, artificial intelligence, or information intermediation shall, as applicable, identify the governmental purpose; identify authorized information domains; define permitted informational acts; prohibit independent or materially unrelated use; prohibit unauthorized aggregation, enrichment, correlation, profiling, inference, sale, licensing, or redisclosure; restrict subcontractors and downstream recipients; establish

retention, return, deletion, and preservation requirements; establish provenance and audit obligations; provide government and authorized oversight bodies sufficient access to assess compliance; require notification of material system, data-source, model, ownership, or processing changes; prohibit contractual provisions that impair rights under this Act; require cooperation with correction, contestability, discovery, and enforcement obligations; provide data and service portability sufficient to prevent avoidable vendor lock-in; require termination or transition procedures that prevent loss of records required for lawful continuity, audit, or enforcement; and expressly incorporate applicable duties under PDTA, VIDA, GAAFA, and implementing FCGIAS requirements.

#### **(d) No Capability Laundering Through Vendor**

A Government Agency may not procure, license, subscribe to, or otherwise obtain through a vendor materially broader Standing Technical Capability than the agency could lawfully maintain itself merely because the capability is bundled, commercially available, proprietary, or operated externally.

#### **(e) Vendor Independent Use**

Where a vendor seeks independently to use, aggregate, enrich, train upon, profile, infer from, sell, license, or redisclose information obtained through a governmental relationship, that activity is outside ordinary government processing authority unless independently authorized by law and compliant with this Act. Nothing in a procurement contract, terms of service, privacy notice, or vendor policy independently supplies such authority.

#### **(f) Governmental Partners**

Information lawfully available to one Government Agency or sovereign does not become generally available to another merely because a memorandum of understanding, data-sharing agreement, common platform, fusion arrangement, task force, grant, cooperative agreement, or technical interface exists. Each governmental participant shall possess independently sufficient authority for its material informational acts.

#### **(g) Intergovernmental Capability Laundering**

A Government Agency may not obtain through another governmental entity or sovereign informational capability that it could not lawfully exercise directly. The authorities of participating governments shall not be aggregated into a collective generalized informational authority unless law independently creates and sufficiently bounds such authority.

#### **(h) Shared Services**

A shared governmental platform may support multiple agencies or purposes where each actor's authority remains distinguishable; Purpose Sequestration is preserved; cross-purpose informational acts require sufficient authorization; administration does not create unrestricted substantive access; metadata does not create unauthorized generalized surveillance capability; and the platform otherwise complies with Section 19.

##### **(h-1) Composite Governmental Information Transactions**

Where a governmental function is performed through a Composite Governmental Information Transaction, the transaction shall be assessed end-to-end. Each participating Government Agency, Vendor, Governmental Actor, intermediary, model, and shared service remains subject to the authority and duty applicable to the role it actually performs. No participant may rely upon fragmentation of custody, processing, contracting, or decision-making to avoid a duty or

prohibition that applies to the composite governmental capability or consequence. End-to-end assessment may identify aggregate technical capability but shall not create aggregate legal authority. Each material informational act within the transaction shall remain independently supportable by authority sufficient for the actor, purpose, Authorized Object, information domain, operation, predicate where applicable, duration, and governmental consequence involved.

#### (h-2) Responsible Government Agency

A Composite Governmental Information Transaction involving more than one Government Agency or material external provider shall identify a Responsible Government Agency unless responsibility is otherwise fixed by law. The Responsible Government Agency shall maintain a current description of the participating actors, purposes, authority, information domains, material operations, authorization transitions, and accountability allocation sufficient to demonstrate conformance. Other participants retain independent obligations applicable to their conduct. Where a shared platform supports multiple governmental functions, responsibility may be allocated in layers: the platform-owning or operating agency may be responsible for shared technical capability, administration, security, logging, and platform conformance, while the Government Agency possessing the substantive governmental function remains responsible for the governmental transaction, programmatic decision, or consequence. RGA designation does not enlarge the authority or access of either layer.

#### (h-3) Role Stacking

Where a person or entity occupies more than one role, including Government Agency, Secondary Information Fiduciary, Vendor, Independent Information Intermediary, Authorized Information Trustee, technical operator, or a specialized statutory role established by VIDA or GAAFA, the duties and restrictions applicable to each actually performed role shall apply cumulatively. Contractual designation or internal organizational label does not control over actual function. Where duties applicable to stacked roles cannot be performed compatibly, the conflict shall not be resolved by disregarding the more protective duty. The transaction or function shall be segregated, restructured, or governed by a more specific controlling law sufficient to resolve the conflict.

#### (h-4) Government-Purpose Model Training and Adaptation

A Government Agency or bounded Vendor may train, fine-tune, adapt, configure, ground, index, embed, retrieve against, or otherwise improve a model or computational system for an authorized governmental purpose only where: (1) Governmental Informational Authority is sufficient for the information and operation involved; (2) the activity is reasonably necessary and sufficiently particular to the governmental function; (3) Purpose Sequestration and applicable use restrictions are preserved; (4) the training or adaptation does not create materially broader cross-purpose Standing Technical Capability; (5) provenance, retention, security, correction, and audit requirements appropriate to the resulting capability are maintained; (6) independent Vendor or commercial reuse is not thereby authorized; and (7) GAAFA applies where the activity concerns an algorithmic, automated, or artificial-intelligence system or material computational artifact. Use of information from more than one governmental purpose for authorized training or adaptation does not merge the participating purposes or authorities and does not by itself authorize deployment or reuse of the resulting model or artifact for another governmental purpose.

#### **(i) Artificial Intelligence and Automated Agents**

An artificial intelligence system or automated agent exercising informational capability for government possesses no independent Governmental Informational Authority; inherits the purpose, authority, scope, domain, operation, duration, and consequence limitations applicable

to the governmental function it serves; may not expand its informational capability merely because expansion improves model performance, predictive accuracy, efficiency, or autonomy; and is additionally subject to GAAFA.

## **Section 18. Access, Processing, Retention, Preservation, and Recovery**

### **(a) Distinct Authorities**

For purposes of this Act, Access Authority determines whether a Governmental Actor may obtain or view information. Active Processing Authority determines whether information may be substantively used, analyzed, correlated, inferred from, disclosed, or acted upon for a governmental purpose. Retention Authority determines whether information may remain maintained within a governmental information environment. Preservation Authority determines whether information must or may be maintained for a legally defined preservation purpose after ordinary Active Processing Authority has expired. Possession of one form of authority does not imply another.

### **(b) Active Processing Authority**

A Government Agency may actively process or use Individual Information or Relational Information only while authority sufficient for that processing or use exists. When active processing authority expires, government shall cease the processing unless independently sufficient authority supports continued activity.

### **(c) Retention**

Information may be retained only for a period supported by the active governmental purpose; reasonably foreseeable adjudication or review; an applicable records-retention requirement; a lawful audit obligation; a lawful preservation requirement; a litigation hold; an evidentiary obligation; archival law; another independently sufficient legal requirement; or a specifically justified operational need consistent with this Act. Retention merely because storage is inexpensive, convenient, potentially useful, or technically automatic is insufficient.

### **(d) Preservation Authority**

Where law requires continued preservation after authority for ordinary processing has expired, the Government Agency shall distinguish preserved information from information available for active operational use. Preservation authority permits retention necessary to satisfy the preservation obligation; does not independently authorize new substantive processing, correlation, inference, disclosure, or reuse; shall be implemented through access restrictions appropriate to the preservation purpose; and terminates when the preservation obligation terminates unless another lawful basis exists.

### **(e) Legal Hold**

Placement of information under legal hold does not create continuing general operational authority over the preserved information. Access to information subject to legal hold shall be limited to the persons, proceedings, and functions lawfully requiring that access.

### **(f) Public Records and Archives**

The fact that information constitutes a public record, archival record, or lawfully accessible record does not by itself create generalized governmental analytical authority. Governmental

correlation, profiling, inference, or construction of materially new individualized knowledge from public or archival records remains subject to this Act. Nothing in this Act requires destruction of information that applicable public-records or archival law requires to be preserved.

#### **(g) Deletion**

Where neither active processing authority nor lawful preservation authority remains, the Government Agency shall delete, destroy, return, or irreversibly place beyond operational use the information as required by law and implementing standards. Deletion requirements shall extend, as appropriate, to working copies, derived operational records, vendor-held copies, caches, replicated environments, and other reasonably accessible operational copies. Backup media may be governed by subsection (h).

#### **(h) Backup and Disaster Recovery**

Backup, disaster-recovery, and continuity systems may retain information beyond ordinary operational retention periods where reasonably necessary for legitimate recovery purposes. Upon restoration: current Governmental Informational Authority governs; expired authority is not revived; information whose active processing authority has expired shall not become generally operational merely because it was restored; current deletion, preservation, correction, and access restrictions shall be reapplied; and restoration processes shall be auditable.

*Data restoration does not restore expired authority.*

#### **(i) Emergency Retention**

Where an emergency lawfully requires temporary expansion of retention or processing, that expansion shall terminate when the emergency authority expires unless an independently sufficient legal basis supports continuation.

#### **(j) Derived Information**

Retention of a Material Derived Inference shall be justified independently from retention of the source information where the inference remains materially capable of affecting an individual. Deletion of source information does not automatically justify indefinite retention of a derived score, classification, inference, or profile.

#### **(k) Statistical Information**

Information that has been transformed into Statistical Information may be retained for legitimate statistical, research, planning, or governmental purposes where the transformation reasonably prevents individualized association, reconstruction, correlation, inference, or action. If later technology or linkage materially restores individualized capability, the information shall no longer be treated as Statistical Information for purposes of the affected use.

## **Section 19. Architectural and Conformance Obligations**

#### **(a) Structural Compliance Required**

A Government Agency shall implement the fiduciary and informational-authority requirements of this Act in architecture, configuration, procurement, authorization mechanisms, operational processes, contracts, or other structural controls where reasonably feasible. Procedural policies alone are insufficient where the system provides ordinary Standing Technical Capability materially broader than the authority Governmental Actors may lawfully exercise.

#### **(b) Authority-Capability Correspondence**

Government information architecture shall cause Standing Technical Informational Capability to correspond to, and not materially exceed, Necessary Standing Informational Capability. Necessary Standing Informational Capability shall remain within Standing Legitimate Informational Authority. A Government Agency shall not maintain materially broader ordinary capability merely because the broader capability is legally available under defined future conditions or because users are instructed not to exercise it.

##### **(b-1) Structural Least Power**

When a legitimate governmental function can reasonably be performed through an architecture that does not create a materially broader standing capability to surveil, correlate, infer, profile, manipulate, or otherwise obtain individualized or relational knowledge, the Government Agency shall use the less informationally powerful architecture unless it documents why the broader standing capability itself is reasonably necessary to the legitimate standing function. In evaluating necessity, the agency shall consider transaction-specific, predicate-activated, segregated, cryptographically bounded, locally verifiable, and other materially less informationally powerful alternatives, together with Utility, Security, reliability, continuity, and lawful operational requirements.

#### **(c) Purpose Sequestration**

Government systems shall preserve functionally meaningful Purpose Sequestration. Purpose Sequestration may be logical rather than physical; may operate within shared infrastructure; shall prevent ordinary cross-purpose access absent sufficient authorization; shall extend to search, APIs, metadata, analytics, artificial intelligence, identity resolution, and other functional means of access; and shall not be defeated through administrative or vendor privilege.

#### **(d) Government Population Golden Record Prohibited**

A Government Agency shall not construct, procure, maintain, or participate in a Government Population Golden Record or functional equivalent as prohibited by Section 14. Assessment shall consider actual informational capability rather than database labels, physical topology, vendor terminology, or organizational ownership.

#### **(e) Authorization Architecture**

Material informational operations shall be authorized according to, as applicable: IDENTITY + GOVERNMENTAL FUNCTION + PURPOSE + AUTHORITY + AUTHORIZED OBJECT + INFORMATION DOMAIN + INFORMATIONAL OPERATION + PREDICATE + DURATION + PERMITTED CONSEQUENCE. An authorization mechanism need not be physically centralized.

#### **(f) Authorization Infrastructure**

An authorization service, identity provider, access-control system, policy engine, audit service, orchestration layer, or comparable infrastructure shall not itself become an unauthorized generalized metadata or informational surveillance system. Authorization metadata shall be minimized to what is reasonably necessary for authorization, security, accountability, and lawful oversight.

#### **(g) Administrative Privilege**

Administrative, maintenance, debugging, security, vendor, recovery, and comparable technical privileges shall be separated from ordinary substantive governmental authority; limited to

persons and systems with a legitimate technical need; independently controlled where the privilege could materially defeat Purpose Sequestration; logged and reviewable; unavailable for ordinary programmatic use; and subject to heightened controls commensurate with the capability.

#### **(h) Break-Glass Capability**

Where emergency, continuity, security, or other legitimate governmental need requires exceptional access, the system may provide break-glass capability only where the exception is defined by purpose, authority, trigger, scope, authorized actor, permitted operations, duration, audit, termination, and subsequent review. Exceptional access shall remain exceptional.

#### **(i) Metadata**

Metadata capable of materially reconstructing a person's activities, relationships, transactions, credential presentations, governmental interactions, or cross-purpose history is subject to this Act according to its informational capability. Metadata shall not be treated as categorically nonpersonal merely because it describes an interaction rather than the underlying content.

##### **(i-1) Learned and Derived Computational Artifacts**

Model weights, embeddings, vector representations, indexes, retrieval stores, feature stores, learned representations, caches, prompts or instruction sets containing material governmental information, and other computational artifacts shall be assessed according to the individualized or relational information, inferential capability, reconstruction capability, and Standing Technical Capability they materially preserve or create. A change in storage format or mathematical representation does not remove an artifact from this Act where government or a person acting for government can reasonably use the artifact to reconstruct, infer, classify, retrieve, associate, or act upon Individual Information or Relational Information.

##### **(i-2) Learned-Artifact Expiration and Reconstitution**

When authority supporting a learned or derived computational artifact expires or materially contracts, the Government Agency shall determine whether the artifact materially preserves individualized, relational, inferential, retrieval, reconstruction, classification, or action capability no longer authorized. If selective removal, effective unlearning, or equivalent contraction is not reasonably practicable, the artifact shall be quarantined from operational use, retired, or retrained or rebuilt from authorized information before further operational use. Distinct lawful Preservation Authority may support preservation of the artifact but does not authorize operational reuse.

#### **(j) Audit Architecture**

Government systems shall maintain audit information sufficient to support accountability, conformance review, investigation of misuse, exercise of rights under this Act where applicable, and enforcement. Audit architecture shall minimize unnecessary cross-purpose individualized surveillance. Nothing in this subsection prohibits independently authorized oversight correlation reasonably necessary to detect insider abuse, systemic violations, cybersecurity threats, or other misconduct.

##### **(j-1) Common Exception Envelope**

Any exception, emergency authority, break-glass capability, temporary variance, special access pathway, extraordinary administrative privilege, or other nonordinary expansion of governmental informational capability recognized under PDTA, VIDA, GAAFA, or binding conformance regulation shall be implemented within an Exception Envelope appropriate to the legal authority involved. An Exception Envelope shall be no broader or longer than the authority supporting it,

shall not convert exceptional capability into ordinary Standing Technical Capability, and shall terminate or contract when the supporting authority terminates or contracts.

#### (j-2) Exception Invocation

An Exception Envelope confers no standing operational permission merely because it has been approved, documented, or technically provisioned. Each invocation shall create an activation record identifying the actual triggering condition; actor or system; Authorized Object or affected scope; permitted operations; activation time; expiration or review time; and accountable official. A class-based Exception Envelope may predefine permissible boundaries only where independently authorized by law, and each invocation remains separately reviewable.

#### (j-3) Immediate Emergency Activation

Where delay necessary to complete the full Exception Envelope would materially threaten life, safety, cybersecurity, continuity of essential government, or another independently recognized exigency, activation may occur upon a minimum record sufficient to identify the existing authority or authority class, triggering condition, actor or system, essential scope, permitted operations, and expiration. Remaining documentation and post-use review shall be completed as soon as reasonably practicable. Where technically practicable, exceptional permissions shall automatically expire or revert to ordinary scope when the authorized period or triggering condition ends.

#### (j-4) Relational Information Downstream Visibility

Relational Information remains subject to this Act throughout collection, verification, correlation, inference, disclosure, retention, automated processing, and governmental action. A Government Agency, Vendor, or automated system shall not avoid an authority, fiduciary, minimization, correction, contestability, retention, or conformance requirement by characterizing information as a relationship, network, household, event, device association, transaction pattern, or other relational artifact rather than as Individual Information. No single Primary Information Trustee has exclusive authority over Relational Information merely because that person is one participant in the relationship. Rights of access, correction, notice, explanation, or contest shall extend to the portion or consequence materially concerning a person, subject to independently applicable rights of other persons, privileges, confidentiality, investigative restrictions, and other law.

##### (j-4.1) Conflicting Relational Interests

Where exercise of an access, correction, explanation, notice, or contest right concerning Relational Information would materially disclose, alter, attribute, or adjudicate information or legal interests concerning another person, the Government Agency shall apply the minimum disclosure and alteration reasonably necessary to vindicate the requesting person's right while protecting third-party information and independently applicable rights. The agency shall preserve provenance for materially competing assertions; identify materially disputed relational information as disputed where reasonably practicable; provide notice to another materially affected person where lawful, reasonably practicable, and not inconsistent with a privilege, protective duty, investigative restriction, safety interest, or other law; and shall not convert one person's materially disputed assertion into an authoritative multi-person fact solely because that person requested correction or supplied the assertion. Before contested Relational Information materially determines an adverse governmental consequence, the agency shall establish the relevant fact or relationship through evidence and a procedure legally appropriate to that consequence. Nothing in this subsection requires disclosure of information that another law lawfully protects from the requesting person.

#### (j-5) Cybersecurity and Abuse-Detection Profile

A Government Agency may conduct cybersecurity, identity-security, fraud-against-system, insider-threat, service-integrity, and abuse-detection processing across otherwise sequestered

technical domains where independently sufficient authority supports the security function and the governmental question or security objective is sufficiently particular. For purposes of this profile, the security function concerns protection of information systems, services, accounts, credentials, authentication or Technical Authorization mechanisms, confidentiality, integrity, availability, resilience, and technical misuse or compromise. Investigation within this profile means investigation of the security incident, compromise, technical misuse, or abuse itself. The profile does not by itself authorize investigation or adjudication of program fraud, personnel misconduct, regulatory violations, criminal conduct, eligibility, benefit entitlement, licensing status, or another substantive governmental matter merely because evidence of that matter is discovered during security processing. Such processing shall be limited to information and operations reasonably necessary to detect, prevent, contain, investigate, remediate, or document the defined security threat or technical abuse; shall minimize substantive program information not necessary to that function; shall preserve provenance and Epistemic Status where outputs may affect a person; and shall not convert security telemetry, audit correlation, anomaly detection, or incident-response capability into standing programmatic, investigative, disciplinary, eligibility, regulatory, or law-enforcement authority. Material transition from the security function to a substantive governmental purpose requires independently sufficient authority for that purpose and Materially Renewed Authorization where required. Emergency security access remains subject to the Exception Envelope. Security and abuse-detection records shall be retained only as authorized and reasonably necessary for security, accountability, evidence, audit, or lawful preservation.

**(j-6) Common Transparency and Protected-Information Rule**

Government Agencies shall provide public and individual transparency sufficient to identify material governmental informational systems and functions, the responsible Government Agency, the general categories of information and informational operations materially used, applicable rights and review mechanisms, and material conformance status, except to the extent disclosure is restricted by independently applicable law. Redaction, delayed notice, or withholding may protect security-sensitive information, privileged material, confidential sources, protected personal or relational information, active investigative information, procurement-sensitive information, trade secrets, and other lawfully protected information, but shall be no broader or longer than reasonably necessary. Agencies shall disclose reasonably segregable nonexempt information sufficient for public accountability. The DTA shall have access to unredacted information reasonably necessary for lawful oversight, subject to applicable security, privilege, and handling restrictions. Public transparency does not itself authorize governmental correlation, inference, disclosure, or reuse.

**(k) Conformance Obligation**

Government Agencies shall comply with binding conformance requirements adopted pursuant to Section 25. Conformance requirements shall implement, but shall not enlarge or diminish, the substantive legal requirements of this Act.

**(l) Conformance Assessment**

Government Agencies shall conduct conformance assessments at times and under circumstances established by regulation, including before material deployment or Material Expansion and periodically thereafter.

**(m) Structural Non-Compensability**

A prohibited structural capability is not rendered conforming solely by encryption, cybersecurity certification, logging, employee training, policy restrictions, privacy notices, contractual

promises, or absence of demonstrated misuse where the prohibited capability remains materially available.

#### **(n) Procurement**

Government shall procure informational functions rather than materially broader generalized informational capability. A material procurement involving Individual Information, Relational Information, identity resolution, analytics, artificial intelligence, commercial information, or intergovernmental interoperability shall be evaluated for the informational capability it makes available to government.

#### **(o) Continuing Obligation**

Architectural conformance is a continuing obligation and shall be reassessed when material changes in information sources, interfaces, identity resolution, artificial intelligence, vendors, commercial information access, intergovernmental access, administrative privilege, or other capability may alter compliance.

## **Section 20. Burdens of Proof and Evidentiary Rules**

#### **(a) Purpose**

The Legislature finds that material evidence concerning governmental informational activity, including system design, authorization, access, metadata, algorithms, contracts, queries, logs, data flows, administrative capabilities, and vendor relationships, is ordinarily within the possession or control of the Secondary Information Fiduciary rather than the affected individual. This section allocates evidentiary burdens accordingly.

#### **(b) Initial Showing by Claimant**

Except as otherwise provided by this Act, a claimant asserting a violation shall make a prima facie showing sufficient to identify the challenged governmental informational act, practice, capability, decision, architecture, or omission and a reasonable basis to believe that the act, practice, capability, decision, architecture, or omission affected the claimant or violated a right enforceable by the claimant. A claimant is not required at the pleading stage to identify confidential technical facts, internal authorizations, source code, undisclosed vendor capabilities, or other information materially within the exclusive control of the Secondary Information Fiduciary.

#### **(c) Burden on Secondary Information Fiduciary**

Upon the showing required by subsection (b), the Government Agency or other person directly subject to the duty at issue bears the burden of establishing compliance with those requirements of this Act for which the material evidence is substantially within its possession or control.

##### **(c-1) Burden for Purpose Divergence and Standing Capability**

For an informational act classified as IJ-2, IJ-3, or IJ-4, the Government Agency bears the burden of documenting the applicable governmental relationship or predicate, Positive Legal Authority, Legitimate Informational Authority, Originating Informational Purpose, degree of Purpose Divergence, necessity, proportionality where applicable, materially less informationally powerful alternatives considered, permitted consequence, duration, structural safeguards, and authorization transition. For Standing Technical Informational Capability, the Government Agency

additionally bears the burden of establishing why the capability itself is reasonably necessary as ordinary standing power rather than being made available only after a predicate or Materially Renewed Authorization.

#### **(d) Government-Citizen Informational Disputes**

In an action challenging an individualized governmental informational act, once the claimant establishes that government performed or materially relied upon the challenged act, the Government Agency bears the burden of establishing the legal and fiduciary authority for that act. The individual does not bear the burden of proving the absence of governmental authority.

#### **(e) Presumptively Disloyal Practices**

For conduct governed by Section 13, the claimant bears the initial burden of establishing that the challenged practice falls within a category described by Section 13(b), and the Secondary Information Fiduciary bears the burden of rebutting the presumption under Section 13(c).

#### **(f) Per Se Disloyal Practices**

For conduct governed by Section 14, once the claimant establishes that the challenged practice materially falls within a prohibited category, the Secondary Information Fiduciary may not defend the practice merely by demonstrating reasonableness, consent, convenience, good faith, security safeguards, or lack of proven consequential harm. The Secondary Information Fiduciary may establish that the challenged capability or practice does not in fact fall within the statutory prohibition; an express exception contained in Section 14 applies; or another controlling law expressly supersedes the prohibition for the specific informational act.

#### **(g) Standard of Proof**

Unless another provision specifies a different standard: (1) civil liability under this Act shall be established by a preponderance of the evidence; (2) rebuttal of a Presumptively Disloyal Practice shall require clear and convincing evidence where the practice materially expands cross-purpose individualized governmental knowledge; (3) a Government Agency relying upon individual authorization to justify a materially contested secondary use shall establish the scope and validity of the authorization by clear and convincing evidence; (4) willfulness, knowing violation, or reckless disregard for purposes of enhanced damages shall be established by clear and convincing evidence; and (5) administrative civil penalties shall be governed by the evidentiary standard otherwise applicable under state administrative law unless this Act provides a higher standard.

#### **(h) Consent or Authorization**

Where government relies upon individual authorization, government bears the burden of proving that the authorization was informed, voluntary, sufficiently particular, and applicable to the challenged informational act; silence, failure to opt out, continued use of a mandatory government service, or acceptance of unrelated terms does not establish authorization; materially bundled authorization shall be construed narrowly against the Secondary Information Fiduciary; and authorization shall not be construed to waive a per se prohibition or to supply governmental authority that cannot lawfully arise from consent.

#### **(i) Recordkeeping Failure**

Where a Secondary Information Fiduciary was required by law to create or maintain a material authorization, audit, provenance, access, retention, or conformance record and fails without

lawful justification to produce that record, a court or enforcement authority may draw an adverse inference that the undocumented requirement was not satisfied. The inference is rebuttable except where destruction or concealment itself constitutes a per se violation under Section 14.

#### **(j) Exclusive Control of Evidence**

Where material evidence necessary to determine compliance is within the exclusive or substantially superior control of a Government Agency, vendor, contractor, intermediary, or automated-system operator, discovery and evidentiary procedures shall be construed to prevent that informational asymmetry from defeating adjudication of rights under this Act.

#### **(k) Trade Secret and Proprietary Claims**

A vendor or Government Agency may not refuse to provide information necessary for judicial, administrative, legislative, inspector-general, or authorized technical review solely on the ground that the information constitutes a trade secret, proprietary information, source code, model information, or confidential business information. A court or authorized body may enter reasonable protective orders necessary to protect legitimate proprietary interests while preserving meaningful review. No contractual proprietary right shall override a Government Agency's obligation to demonstrate compliance with this Act.

#### **(l) Algorithmic and Automated Systems**

Where an artificial intelligence system or Automated Decision System materially contributes to a challenged informational act or governmental consequence, characterization of the system as advisory does not alter the burden imposed by this section; government bears responsibility for establishing the authority, purpose, material inputs, material operations, and permitted use of the system; the absence of complete explainability does not shift the burden to the affected individual; and additional requirements of GAAFA apply.

#### **(m) Structural Capability Evidence**

Evidence that a system was technically capable of performing an informational act does not by itself establish that the act occurred. However, where the claim concerns prohibited Standing Technical Capability, architectural nonconformance, a Government Population Golden Record, Functional Universal Search, unbounded administrative access, or another structural prohibition, actual misuse need not be shown if the prohibited capability itself is established.

#### **(n) Statutory Injury and Consequential Harm**

A violation of a substantive right expressly conferred upon a person by this Act constitutes statutory injury for purposes of a cause of action in the courts of [Enacting State] to the fullest extent permitted by the Constitution and standing law of [Enacting State]. Where this Act makes a fiduciary violation or prohibited structural capability independently actionable, separate consequential economic or physical injury is not an element of the statutory violation unless expressly required. Nothing in this subsection purports to alter the requirements of Article III of the United States Constitution, determines whether a particular claimant possesses standing in federal court, creates standing inconsistent with the Constitution of [Enacting State], or eliminates the requirement that a claimant satisfy subsection (b).

#### **(o) Good Faith**

Good-faith reliance upon legal advice, a vendor representation, an existing policy, or prior governmental practice may be considered in determining enhanced damages or penalties where

permitted by this Act. Good faith does not create Governmental Informational Authority; cure a structural prohibition; rebut a per se violation; eliminate the right to injunctive or structural relief; or prevent correction of an unlawful governmental capability.

#### **(p) Continuing Violations**

A prohibited Standing Technical Capability, unlawful retention, unlawful ongoing processing, unlawful access arrangement, or other continuing informational condition constitutes a continuing violation for purposes of prospective equitable relief until the capability or condition is remediated. The treatment of such conduct for statutory damages and limitations periods shall be governed by Sections 21 and 22.

#### **(q) Trilogy Application**

This section applies to a claim or administrative enforcement proceeding under VIDA or GAAFA to the extent the claim requires proof of Governmental Informational Authority, purpose, particularity, necessity, Material Expansion, informational operation, Vendor or intermediary authority, architectural capability, conformance, or another matter governed by this Act, unless VIDA or GAAFA expressly establishes a different burden or evidentiary rule for the specific claim.

## **Section 21. Private Right of Action**

#### **(a) Civil Action Authorized**

A person aggrieved by a violation of this Act, or by a violation of VIDA or GAAFA that the applicable Act expressly makes enforceable through this section, may bring a civil action in [appropriate court] against:

- (1) a Government Agency responsible for the violation;
- (2) a Secondary Information Fiduciary responsible for the violation;
- (3) a contractor, vendor, Independent Information Intermediary, or other nongovernmental person directly liable under this Act; or
- (4) multiple responsible persons where the challenged informational activity involved joint, coordinated, delegated, or composite conduct.

An action may seek declaratory, injunctive, equitable, mandamus, monetary, or other relief authorized by this Act.

For purposes of this section, a person is “aggrieved” where the person alleges a violation of a substantive right conferred upon that person by this Act and satisfies the standing requirements applicable in the forum in which the action is brought.

#### **(a-1) Downstream Enforceable Right**

A civil action under this section may be maintained for a violation of VIDA or GAAFA only where the applicable Act: (1) expressly creates an individual right or protection enforceable through this section; (2) prohibits an informational act, architectural capability, automated operation, or covered commercial practice and the claimant satisfies the statutory nexus and standing requirements; or (3) expressly imposes a privately enforceable duty upon a Vendor or Commercial Participant. A provision governing agency administration, regulator organization, rulemaking, procurement procedure, reporting, registry maintenance, assessment filing, periodic review, or another institutional process does not create a standalone private claim unless the applicable Act expressly so provides. Failure to comply with such a provision may constitute evidence of, or support relief for, an independently enforceable violation.

#### **(b) Actionable Violations**

An action may be maintained for, among other things:

- (1) breach of a fiduciary duty established by Section 7;
- (2) violation of a right established by Section 15;
- (3) unauthorized governmental informational activity;
- (4) Material Expansion without Materially Renewed Authorization;
- (5) violation of Purpose Particularity or Question Particularity requirements;
- (6) unlawful Material Secondary Correlation;
- (7) unlawful Material Derived Inference;
- (8) unlawful Bounded Government Discovery or Generalized Discovery;
- (9) unlawful Independent Information Intermediation;
- (10) a Presumptively Disloyal Practice not successfully rebutted;
- (11) a Per Se Disloyal Practice;
- (12) unlawful retention, processing, disclosure, or preservation;
- (13) failure to satisfy architectural or conformance requirements;
- (14) failure to honor notice, correction, access, explanation, revocation, portability, or contestability rights;
- (15) failure to maintain required authorization, provenance, audit, or conformance records;
- (16) retaliation against a person for exercising a right under this Act; or
- (17) another violation expressly made enforceable by this Act.

#### **(c) No Administrative Exhaustion**

A claimant is not required to exhaust an administrative complaint, appeal, enforcement, audit, or other remedy before bringing an action under this section.

A person may simultaneously or successively pursue relief before the Data Trusteeship Authority, another authorized administrative body, the Attorney General, and a court under this section, subject to ordinary rules governing claim preclusion, satisfaction of judgments, and prevention of duplicative recovery.

#### **(d) Nonwaiver**

No agreement may waive or materially diminish:

- (1) a substantive right established by this Act;
- (2) a fiduciary duty established by this Act;
- (3) Governmental Informational Authority limitations;
- (4) a statutory remedy;
- (5) DTA or Attorney General enforcement authority;
- (6) a Government Agency's conformance obligation; or
- (7) another substantive protection made nonwaivable by this Act.

An agreement governing the forum or procedure for resolution of a claim, including an arbitration agreement or representative-action waiver, is enforceable only to the extent required or permitted by applicable federal and state law.

Nothing in such an agreement may be construed to enlarge Governmental Informational Authority or reduce the substantive obligations imposed by this Act.

#### **(e) Limitations Period**

An action under this Act shall be commenced within [five years] after the latest of:

- (1) the date of the violation;
- (2) the date the claimant discovered or reasonably should have discovered the violation;
- (3) the date a concealed informational practice became reasonably discoverable;
- (4) the date a Government Agency was required to disclose a material informational act and failed to do so; or
- (5) for a continuing violation, the date the challenged continuing condition ceased, subject to subsection (f).

#### **(f) Continuing Violations**

For prospective equitable relief, a prohibited Standing Technical Capability, unlawful processing arrangement, unlawful retention condition, unlawful access capability, or other continuing informational condition remains actionable while the condition continues.

For monetary relief, a court shall avoid treating every automated query, replicated record, or technical event arising from the same continuing architectural condition as a separate violation unless the Legislature has expressly prescribed such treatment. Nothing in this subsection prevents recovery for distinct material informational acts or distinct harms.

#### **(g) Concealment and Tolling**

The limitations period shall be tolled during any period in which a defendant knowingly conceals a material informational practice or fails to make a disclosure expressly required by law where the concealment or failure materially prevents discovery of the claim.

#### **(h) Representative and Class Actions**

Actions may be maintained individually or, where the applicable procedural requirements are satisfied, on behalf of a class or other representative group.

Where a claimant establishes that substantially the same challenged system, architectural capability, policy, model, contract, informational practice, or authorization defect materially affected a class of persons, the court shall consider the common systemic character of the violation in determining whether representative adjudication is appropriate. Nothing in this Act eliminates constitutional or procedural requirements governing class actions.

#### **(i) Cumulative Rights**

The private right of action established by this section is cumulative and does not supersede or limit a right of action available under VIDA, GAAFA, the Constitution of the United States, the Constitution of [Enacting State], applicable civil-rights law, state privacy, public-records, consumer-protection, administrative, tort, contract, or fiduciary law, or another applicable source of law. Claims arising from the same conduct may be joined where otherwise permitted.

#### **(j) No Retaliation**

A Government Agency, Secondary Information Fiduciary, contractor, vendor, or other person may not retaliate against an individual for exercising a right under this Act, filing or supporting a complaint, seeking correction or explanation, participating in an investigation or audit, providing

information to an enforcement authority, or refusing an informational use that depends solely upon voluntary authorization. Retaliation constitutes an independent violation.

**(k) Trilogy Procedure**

Unless VIDA or GAAFA expressly provides otherwise for a specific claim, subsections (c) through (j) of this section govern a civil action brought through this section for a violation of VIDA or GAAFA.

## **Section 22. Remedies**

### **(a) General Remedial Principle**

A court shall have authority to grant relief sufficient to stop the unlawful informational act, remove or constrain unlawful informational capability, restore lawful informational boundaries, correct or qualify materially inaccurate information, compensate actual injury where proven, vindicate statutory rights where statutory damages are authorized, deter knowing, reckless, or willful violations, and prevent recurrence.

Remedies shall address the informational capability or relationship giving rise to the violation and not merely the last observable misuse.

### **(b) Declaratory Relief**

A court may declare the existence or absence of Governmental Informational Authority, the lawful scope of an Originating Informational Purpose, whether Material Expansion occurred, whether an informational capability violates this Act, whether an informational practice is presumptively or per se disloyal, or the rights and duties of parties under this Act.

### **(c) Injunctive and Structural Relief**

A court may order:

- (1) cessation of unlawful processing;
- (2) cessation of unlawful collection or acquisition;
- (3) deletion where legally appropriate;
- (4) segregation or sequestration of information;
- (5) revocation or narrowing of access;
- (6) suspension of a system, interface, API, model, query capability, subscription, or vendor service;
- (7) modification of system architecture;
- (8) removal of generalized search or identity-resolution capability;
- (9) termination or restructuring of a data-sharing arrangement;
- (10) termination or restructuring of a government-to-intermediary disclosure, intermediary-to-government acquisition, or Government-Intermediary Reacquisition Architecture;
- (11) implementation of Authorization Friction;
- (12) restoration of Purpose Sequestration;
- (13) correction, invalidation, supersession, or qualification of materially inaccurate information or inferences;
- (14) reprocessing or reconsideration of an affected governmental decision;

- (15) additional auditing or conformance review;
- (16) notification to materially affected persons;
- (17) destruction or restriction of unlawfully generated derivative information where legally appropriate; or
- (18) another structural measure reasonably necessary to restore compliance.

#### **(d) Least-Power Remediation**

Where multiple structural remedies could restore compliance, a court should ordinarily proceed according to the following hierarchy to the extent appropriate:

*REMOVE PROHIBITED CAPABILITY → NARROW CAPABILITY → TRANSACTIONALIZE ACCESS → REQUIRE MATERIALLY RENEWED AUTHORIZATION → SEGREGATE OR SEQUESTER → MONITOR AND AUDIT RESIDUAL CAPABILITY.*

Audit or training alone shall not be treated as sufficient remediation where prohibited Standing Technical Capability remains materially intact.

#### **(e) Mandamus**

A court may issue mandamus or comparable mandatory relief to compel performance of a nondiscretionary obligation under this Act, including access, correction, revocation, required conformance assessment, cessation of expired processing authority, production of records required for review, or another mandatory statutory duty.

#### **(f) Compensatory Damages**

A successful claimant may recover compensatory damages for proven injury proximately caused by a violation, including where applicable economic loss; denial or delay of benefits or services; loss of employment, licensing, educational, housing, contractual, or comparable opportunity; costs incurred correcting an informational error; injury arising from unauthorized disclosure or misuse; legally cognizable reputational, emotional, or dignitary injury; injury resulting from unlawful surveillance, profiling, discrimination, or automated governmental action; and other legally cognizable harm.

#### **(g) Statutory Damages**

A claimant who establishes an actionable violation but cannot establish or quantify actual monetary loss may recover statutory damages of not less than [\$1,000] for a material violation, subject to legislative specification.

In determining the amount of statutory damages within any prescribed range, the court may consider the nature of the right violated; sensitivity of the information; scope of the informational capability; number of information domains involved; duration; degree of culpability; whether the violation was structural or transactional; concealment; number of persons materially affected; remedial action; prior violations; and deterrence. The Legislature may establish caps, floors, aggregate limitations, or alternative schedules appropriate to public and private defendants.

#### **(h) Continuing-Violation Damages**

The Legislature may provide statutory damages of [\$\_\_\_] per day after a final judicial or administrative determination, actual notice of a clearly established violation, or expiration of a reasonable remediation period ordered by a court or enforcement authority, for failure to remediate a continuing violation.

A daily-damages provision should not apply before a defendant has a reasonably ascertainable obligation and opportunity to cure unless the violation is knowing or willful.

#### **(i) Enhanced Damages**

Where authorized by the law of [Enacting State], a court may award enhanced or punitive damages against a nongovernmental defendant for willful, malicious, fraudulent, or reckless violation of this Act. Enhanced monetary remedies against Government Agencies and public employees shall be governed by subsections (m) through (o) and other applicable state law.

#### **(j) Attorneys' Fees and Costs**

A prevailing claimant shall be entitled to reasonable attorneys' fees and costs. A prevailing defendant may recover attorneys' fees only where the court finds that the claimant's action was frivolous, brought in bad faith, or maintained after it became objectively clear that no reasonable basis existed.

#### **(k) Emergency Relief**

Courts shall provide procedures for expedited temporary or preliminary relief where a claimant demonstrates a substantial likelihood of ongoing unlawful surveillance, imminent unauthorized disclosure, continuing use of materially inaccurate information producing adverse action, irreversible correlation or inference, imminent destruction of evidence, operation of a prohibited generalized informational capability, or another informational harm for which later damages would be materially inadequate.

#### **(l) Reopener Relief**

Where a governmental determination was materially affected by information, correlation, inference, model output, or processing found unlawful under this Act, a court may order de novo reconsideration, independent human review, reconsideration using corrected information, exclusion of unlawfully obtained or improperly characterized informational artifacts where required by law, or other appropriate process sufficient to remedy the effect of the violation.

#### **(m) State Consent to Suit**

To the fullest extent permitted by the Constitution of [Enacting State], the State consents to suit under this Act in the courts of [Enacting State] for declaratory, injunctive, mandamus, structural, and monetary relief expressly authorized by this Act, subject to limitations expressly enacted by the Legislature.

The Legislature shall specify before enactment monetary liability limits, if any; judgment-payment procedures; application to political subdivisions; any required notice-of-claim procedures; execution and payment procedures; and any other conditions constitutionally necessary to effectuate the waiver.

Nothing in this Act constitutes consent by [Enacting State] to suit against the State in federal court unless the Legislature expressly so provides. Sovereign immunity shall not bar prospective relief against a Government Agency in the courts of [Enacting State] to the extent expressly authorized by this Act and permitted by the Constitution of [Enacting State].

#### **(n) Institutional Budget Accountability**

To the extent permitted by the Constitution, appropriations law, federal funding restrictions, judgment-payment law, and other controlling fiscal law of [Enacting State], monetary penalties and court-ordered payments attributable to a Government Agency's violation should be charged

to or reflected against the budgetary responsibility of the agency whose informational architecture or conduct caused the violation rather than being absorbed without consequence by a general statewide liability mechanism.

The Legislature shall establish implementing fiscal procedures that preserve institutional accountability, do not unlawfully impair federally restricted funds or constitutionally protected expenditures, preserve essential governmental services, identify the responsible agency, and make the fiscal consequence of repeated or structural nonconformance visible to appropriating authorities. Nothing in this subsection independently authorizes expenditure without lawful appropriation.

#### **(o) Public Employee Responsibility**

Ordinary institutional or architectural nonconformance shall be remedied against the responsible Government Agency and shall not, without more, create personal monetary liability for an individual public officer or employee.

A public officer or employee may be personally liable only where this Act or another law expressly provides personal liability for knowing or willful conduct, including deliberate unauthorized sale or disclosure; deliberate purpose laundering; intentional falsification or concealment of required audit or authorization records; retaliatory informational use; intentional circumvention of a final judicial or DTA order; or another knowing or willful violation expressly designated by law.

Public funds shall not be used to indemnify punitive or enhanced damages imposed personally upon an officer or employee following a final finding of conduct described in this subsection, except where controlling law requires otherwise.

#### **(p) No Double Recovery**

A claimant may pursue cumulative claims under PDTA, VIDA, GAAFA, and other law but may not obtain duplicative monetary recovery for the same injury.

#### **(q) Trilogy Remedies**

The remedies in this section are available for a violation of VIDA or GAAFA made enforceable through Section 21, subject to any more specific remedial limitation or remedy expressly established by the applicable Act. A court shall avoid duplicative recovery for the same injury but may combine structural remedies necessary to cure a composite violation.

## **Section 23. Data Trusteeship Authority and Enforcement**

### **(a) Data Trusteeship Authority**

There is established an independent Data Trusteeship Authority, referred to in this Act as the "DTA."

The DTA is the principal independent oversight and enforcement authority for PDTA, VIDA, and GAAFA.

The DTA shall maintain specialized institutional capacity for:

- (1) fiduciary and informational-authority enforcement;
- (2) identity, credential, verification, interoperability, and information-architecture conformance under VIDA; and

(3) artificial intelligence, algorithmic, automated-decision, model-governance, and agentic-system oversight under GAAFA.

Nothing in this subsection requires the DTA to consolidate operational government information or create a common informational repository. Oversight consolidation shall not constitute informational integration.

#### **(b) Primary Functions**

The DTA shall receive and investigate complaints; conduct proactive audits without requiring a prior complaint; conduct or commission architectural and technical conformance reviews; investigate fiduciary and structural violations; oversee implementation of binding conformance regulations under Section 25; issue interpretive guidance consistent with this Act; coordinate enforcement across PDTA, VIDA, and GAAFA; provide technical assistance to Government Agencies; support individuals in exercising rights; and report to the Legislature as required by subsection (m).

#### **(c) Investigative Authority**

The DTA may, subject to applicable law, issue subpoenas for documents, testimony, records, contracts, system documentation, architecture diagrams, data-flow information, access records, model documentation, and other relevant evidence; require production of conformance assessments; inspect or test covered governmental systems; conduct negative-capability testing; obtain access to technical personnel and responsible officials; obtain information from contractors, vendors, and Independent Information Intermediaries performing covered functions; require preservation of relevant evidence; and retain independent technical experts.

#### **(d) Proprietary Systems and Protected Information**

A vendor's assertion of trade secret, proprietary, confidential, or intellectual-property protection shall not prevent the DTA from obtaining information reasonably necessary to assess compliance. The DTA shall protect legitimate confidential commercial information, protected government information, system-security information, and Individual Information from unnecessary disclosure consistent with law.

#### **(e) Administrative Orders**

Following procedures required by state administrative law, the DTA may issue cease-and-desist orders; corrective-action orders; access-restriction orders; processing-suspension orders; remediation orders; conformance-assessment orders; system-modification orders; deletion, sequestration, or preservation orders where legally appropriate; vendor or procurement remediation requirements; and other orders authorized by law.

#### **(f) Civil Administrative Penalties**

The DTA may impose civil penalties up to [\$\_\_\_] for a material negligent violation; [\$\_\_\_] for a knowing or reckless violation; [\$\_\_\_] for a per se violation; [\$\_\_\_] per day for knowing failure to comply with a final DTA remediation order; and another amount specified by the Legislature.

In determining a penalty, the DTA shall consider the nature and sensitivity of the information, scope and duration of the capability or practice, degree of culpability, number of persons affected, concealment, remediation, prior violations, and deterrence.

### **(g) Structural Violations**

Where a violation concerns prohibited Standing Technical Capability or another structural defect, the DTA shall prioritize elimination or restructuring of the offending capability over imposition of monetary penalties alone.

### **(h) Attorney General Authority**

The Attorney General shall have concurrent authority to enforce this Act and may bring an action in the name of the State; seek declaratory, injunctive, structural, and monetary relief; enforce DTA subpoenas or orders; pursue claims on behalf of residents where authorized by law; coordinate with other states and federal authorities; and pursue any other remedy available under state law. The DTA may refer matters to the Attorney General.

### **(i) Criminal Referral**

Where the DTA has reasonable grounds to believe evidence establishes criminal conduct, including intentional destruction of evidence, unlawful sale of protected government information, bribery, unauthorized computer access, fraudulent concealment, or another offense, the DTA shall refer the matter to the appropriate prosecuting authority. Nothing in this Act independently creates a criminal offense unless expressly provided.

### **(j) Coordination**

The DTA shall coordinate with the Attorney General, inspectors general, state auditors, procurement authorities, cybersecurity authorities, archives and records officials, civil-rights authorities, consumer-protection authorities, and other entities possessing independent jurisdiction.

VIDA and GAAFA shall not establish a separate general-purpose informational oversight body duplicating the DTA's jurisdiction. Specialized advisory panels, technical boards, or review bodies may be established within or in coordination with the DTA without displacing the DTA's principal enforcement authority.

Coordination shall not create generalized access to Individual Information beyond the authority of the participating body.

#### **(j-1) Remedial and Operational Boundary**

The DTA determines legal and conformance requirements and may order remediation necessary to cure a violation, including required capability outcomes, access restrictions, purpose boundaries, testing, suspension, or removal of prohibited capability. Except where necessary to enforce a final lawful order or where enacted law expressly provides otherwise, the DTA shall not select ordinary executive technology products, direct day-to-day system administration, operate agency information systems, or substitute itself for the operational authority of the State CIO or responsible Government Agency. The State CIO and Responsible Government Agency retain authority to select and implement a lawful technical means of satisfying the required conformance outcome, subject to DTA review of whether the resulting implementation conforms.

### **(k) Complaints**

The DTA shall provide an accessible process for filing complaints that does not require technical expertise; permits representation by an Authorized Information Trustee or counsel; provides reasonable accommodation; supports individuals with limited English proficiency or limited digital access; protects complainants against retaliation; and permits confidential treatment where required by law.

### **(l) Public Guidance and Assistance**

The DTA shall publish guidance explaining rights under this Act; model governmental purpose statements; guidance on Purpose Particularity and Question Particularity; model contract clauses; conformance guidance; descriptions of prohibited structural capabilities; complaint procedures; and anonymized or appropriately redacted enforcement decisions.

### **(m) Annual Report**

At least annually, the DTA shall report publicly and to [Legislative Body] concerning complaints received and resolved; audits conducted; conformance findings; structural violations identified; enforcement actions; civil penalties; Government Population Golden Record or equivalent risks; significant uses of Independent Information Intermediaries; major developments in AI or automated informational capability; intergovernmental information-sharing risks; recurring implementation problems; expenditures and staffing; recommended legislative amendments; and coordination across PDTA, VIDA, and GAAFA. Reports shall not disclose protected Individual Information or compromise lawful investigations.

### **(n) Institutional Independence**

The Legislature shall provide the DTA with institutional safeguards sufficient to permit meaningful review of agencies whose information architecture it regulates. Such safeguards may include fixed terms for leadership; removal only for cause; independent budget presentation; authority to hire technical and legal personnel; restrictions on conflicts of interest; restrictions on immediate employment with regulated technology vendors; and direct reporting authority to the Legislature.

### **(o) Funding**

The Legislature shall provide appropriations reasonably sufficient for DTA staffing; technical assessment capability; public education; legal and technical assistance to individuals; conformance testing; development and maintenance of implementing standards; coordination with VIDA and GAAFA implementation; and grants or assistance necessary to help state and local agencies remediate legacy systems.

Implementation funding should favor remediation that reduces generalized informational capability rather than merely adding compliance documentation to existing architecture.

### **(p) Constitutional Branches**

The substantive principles of this Act apply throughout state government to the fullest extent permitted by the Constitution of [Enacting State].

The DTA's compulsory administrative authority under this section applies directly to executive-branch agencies and political subdivisions subject to state legislative regulation.

The judicial and legislative branches shall adopt functionally equivalent rules and institutional mechanisms implementing the substantive requirements of this Act with respect to their own informational activities, consistent with constitutional separation of powers.

Nothing in this Act authorizes an executive or independent administrative body to direct the adjudicative functions of a court; obtain information protected by judicial privilege or constitutional judicial independence; direct the internal legislative functions of the Legislature; compel disclosure protected by legislative privilege; or exercise authority inconsistent with constitutional separation of powers.

Where a dispute concerning compliance by a constitutional branch cannot be resolved through the applicable branch-specific mechanism, relief may be sought through a judicial proceeding authorized by law.

## **Section 24. Relationship to VIDA, GAAFA, and Other Law**

### **(a) Coordinated Trilogy**

This Act shall be construed in harmony with the Verifiable Identity and Digital Autonomy Act and the Government Algorithmic Accountability and AI Fiduciary Act. Together, the three Acts establish a coordinated statutory framework for governmental informational authority.

### **(b) Functional Allocation**

Unless otherwise expressly provided:

- (1) PDTA establishes the legal and fiduciary relationship governing governmental informational power, including authority, purpose, rights, duties, presumptions, burdens, and remedies;
- (2) VIDA governs implementation of identity, credential, verification, interoperability, information-sequestration, and related governmental information architecture; and
- (3) GAAFA governs artificial intelligence, algorithmic inference, automated decision systems, agentic systems, model governance, provenance, contestability, and computational exercise of governmental informational power.

### **(c) Same Authority Model**

VIDA and GAAFA shall be interpreted consistently with the principles that possession does not create authority; technical capability does not create authority; commercial availability does not create authority; predictive utility does not create authority; Material Expansion requires Materially Renewed Authorization; lawful interoperability does not create generalized informational authority; artificial intelligence possesses no governmental authority independent of the governmental function it serves; and government may not outsource a constitutional, fiduciary, or architectural violation.

### **(d) Conflict**

Where provisions of PDTA, VIDA, and GAAFA can reasonably be read consistently, they shall be read together.

Where an irreconcilable conflict exists:

- (1) a provision expressly governing the more specific informational act controls over a general provision;
- (2) a provision imposing a constitutionally required higher protection controls;
- (3) a later enactment shall not be construed by implication to diminish protections established by this Act where the statutes can reasonably be harmonized; and
- (4) no ambiguity shall be construed to create Governmental Informational Authority by implication; and
- (5) broad authorization to perform a governmental function shall not by implication repeal, waive, or satisfy a more specific informational-legitimacy, Purpose-Divergence, or Structural Least-Power requirement of this Act.

#### **(e) No Automatic Greater-Protection Rule Where Authority Differs**

A court shall not mechanically resolve every conflict by selecting the provision that appears more restrictive in isolation where doing so would defeat independently lawful governmental authority or the carefully bounded authorization structure established by this Act. The governing inquiry is whether the statutes can be harmonized to preserve both legitimate governmental authority and the strongest protection consistent with that authority.

#### **(f) Other Rights Preserved**

Nothing in this Act limits rights or remedies available under the United States Constitution; the Constitution of [Enacting State]; civil-rights law; public-records law; records-management and archival law; administrative-procedure law; consumer-protection law; other privacy law; common-law fiduciary, tort, contract, property, or equitable principles where applicable; or another applicable law.

#### **(g) More Protective Law**

Nothing in this Act prevents another statute from imposing a more protective requirement upon a defined governmental informational activity, including a warrant requirement, categorical prohibition, shorter retention period, stricter minimization rule, or more protective individual right.

#### **(h) No Implied Expansion**

No provision of this Act, VIDA, or GAAFA shall be construed as an affirmative grant of governmental authority merely because the statute regulates how a governmental informational act must be performed. Compliance requirements constrain otherwise lawful authority; they do not create authority absent an independent legal basis.

#### **(i) Procedural Spine**

Where VIDA or GAAFA makes a violation enforceable through PDTA, PDTA supplies the generally applicable burdens, procedure, enforcement mechanisms, and remedies unless the downstream Act expressly provides a more specific rule. This subsection does not create a cause of action for a downstream provision that the Legislature has not made privately enforceable.

## **Section 25. Rulemaking and FCGIAS Conformance**

#### **(a) Rulemaking Authority**

The DTA, in consultation with [Chief Information Officer], the Attorney General, affected state and local agencies, and other appropriate stakeholders, shall adopt rules necessary to implement this Act.

#### **(b) Initial Conformance Standard**

The DTA shall use the Fiduciary Commons Government Information Architecture Standard, Version 2.1, as the initial technical reference for development of binding conformance regulations implementing this Act.

FCGIAS does not independently create law merely by publication. Binding obligations arise from this Act, VIDA, GAAFA, and regulations lawfully adopted by the DTA.

### **(c) Public Adoption**

A technical standard, control, methodology, or portion of FCGIAS incorporated into a binding regulation shall be publicly identified; version-controlled; available to the public without charge; adopted through the notice-and-comment procedures applicable under [State Administrative Procedure Act]; accompanied by a description of material changes from the preceding binding version; and maintained in an accessible public archive.

#### **(c-1) Trilogy Conformance Code and Version Registry**

The DTA shall maintain the binding conformance requirements adopted under PDTA, VIDA, and GAAFA as a coordinated Trilogy Conformance Code. The DTA shall maintain a public version registry identifying: (1) each current binding provision; (2) the statutory authority implemented; (3) the applicable FCGIAS or other technical source, if any; (4) the effective date; (5) superseded versions; (6) material changes; (7) implementation classifications or conformance profiles; and (8) any active transition provision or variance affecting the requirement. A Government Agency or Vendor shall not be required to infer the binding conformance rule from multiple inconsistent versions or unofficial technical publications.

#### **(c-2) FCGIAS Reference Integrity and Statutory Traceability**

Every binding technical control, conformance test, implementation classification, or incorporated FCGIAS provision shall identify the specific enacted statutory provision containing the duty, prohibition, right, exception, or administrative function it implements and shall be reasonably necessary to implement that operative provision. Mere consistency with a broad statutory principle, policy desirability, administrative convenience, or greater protectiveness is insufficient to create a binding requirement. The DTA shall not make an FCGIAS provision or other technical requirement binding where the requirement materially adds to, changes, or substitutes for the operative substantive rule enacted by the Legislature. A material substantive change identified as desirable through FCGIAS, conformance experience, or the Normative Traceability Matrix shall be treated as a legislative recommendation unless independently sufficient enacted authority already exists. An FCGIAS publication, candidate standard, successor version, explanatory appendix, reference implementation, control catalog, or Normative Traceability Matrix is non-self-executing unless and until a specifically identified portion is lawfully incorporated into the Trilogy Conformance Code under this standard. If FCGIAS or another technical source conflicts with the Constitution, enacted law, or a valid controlling regulation, the higher legal authority governs. A technical source may be more protective as guidance, but it may not create a mandatory substantive restriction, exception, governmental power, private cause of action, evidentiary burden, or remedy absent independently sufficient enacted authority.

### **(d) Governmental Decision Authority**

No privately maintained, externally modified, or subsequently published version of FCGIAS becomes binding merely because it bears the FCGIAS name. The DTA shall retain final governmental authority over every binding conformance requirement.

### **(e) Appropriate Technical Subjects**

Binding conformance regulations may address assessment methodology; conformance evidence; Authority-Capability Delta assessment; Authorization Friction classifications; negative-capability testing; red-team testing; Structural Disqualifier assessment; authorization-transaction documentation; Bounded Government Discovery controls; Purpose-Bounded Analytics Enclaves; administrative and break-glass controls; audit implementation; procurement specifications; certification; interoperability; technical implementation patterns; and other matters implementing substantive law.

#### **(f) Substantive Limits**

Neither FCGIAS nor a DTA regulation may, without legislative authorization, create Positive Legal Authority or Governmental Informational Authority; declare informational power legitimate merely because a competent source has authorized the underlying governmental function; relax the statutory criteria for Legitimate Informational Authority, Purpose Divergence, Informational Justification, Necessary Standing Informational Capability, or Structural Least Power; eliminate or materially diminish a substantive right or fiduciary duty; convert a statutory per se prohibition into a rebuttable presumption; materially broaden a statutory exception; eliminate or restrict the private right of action; reduce a statutory evidentiary burden; create a new category of personal monetary liability; or otherwise alter substantive law rather than implement it.

##### **(f-1) No Conformance Bootstrap**

A statute, regulation, administrative authorization, contract, policy, technical permission, procurement instrument, or other governmental act does not establish conformance merely because it authorizes the capability being evaluated. Conformance under this Act requires application of the enacted legitimacy and structural criteria to the capability's source, scope, purpose, necessity, consequence, duration, and standing availability.

##### **(f-2) Later Legislative Departure**

A later enacted statute may expressly supersede a requirement of this Act to the extent constitutionally valid. Implied repeal, waiver, or satisfaction of a specific informational-legitimacy or structural requirement shall not be inferred solely from broad statutory purpose language or generalized authorization to perform a governmental function.

#### **(g) Successor Standards**

The DTA may update binding conformance regulations in response to technical developments, implementation experience, new circumvention mechanisms, changes in interoperability, security developments, or new forms of functional informational integration, provided the changes remain within subsection (f).

#### **(h) Technology Neutrality**

Rules shall be technology-neutral but may be architecture-specific. No rule shall require a particular commercial technology, vendor, blockchain, wallet, credential standard, cloud provider, identity protocol, artificial intelligence model, cryptographic system, or other product unless procurement law independently justifies such specification. Rules may recognize compliant technical approaches, including decentralized credentials, cryptographic verification, Zero Trust architectures, federated authorization, and other technologies.

#### **(i) Procurement Integration**

The State procurement authority shall incorporate applicable PDTA and binding conformance requirements into procurement rules, solicitations, contracts, renewals, and vendor assessments.

#### **(j) Local Government**

The DTA shall adopt implementation schedules and technical assistance appropriate to local governments, taking account of system size, fiscal capacity, legacy technology, shared-service dependencies, and risk presented by the informational capability. No local-government exception may permit a prohibited structural capability to become permanently exempt solely because remediation is costly.

### **(k) Waivers and Transitional Variances**

A temporary implementation variance may be granted for good cause where immediate full conformance is technically or operationally impracticable; the Government Agency identifies the specific nonconformance; no Per Se Disloyal Practice is authorized by the variance unless expressly permitted by statute; interim controls materially reduce risk; a remediation plan and schedule are approved; the variance is public except to the extent lawfully confidential; the variance expires automatically; and renewal requires a new showing. A variance does not create permanent Governmental Informational Authority.

#### **(k-1) Exception Envelope for Variances and Specialized Exceptions**

A variance or specialized conformance exception granted under this section shall identify and remain within an Exception Envelope. The DTA may specify documentation and technical controls necessary to make the envelope reviewable and enforceable but may not use the envelope to supply missing Governmental Informational Authority or enlarge a statutory exception.

### **(l) Education and Assistance**

The DTA shall provide model policies, implementation guidance, training, and technical resources to facilitate compliance.

## **Section 26. Periodic Review**

#### **(a) Consolidated Trilogy Review**

At least once every [five] years after the effective date, the DTA, in consultation with the State CIO, Attorney General, affected state and local agencies, and appropriate public stakeholders, shall conduct one coordinated review of PDTA, VIDA, GAAFA, the Trilogy Conformance Code, and the use of FCGIAS as a technical reference, and shall report recommended statutory or regulatory changes to [Legislative Body]. VIDA and GAAFA may specify specialized review subjects but shall not require a duplicative general review cycle.

#### **(b) Required Subjects**

The coordinated review shall assess at minimum: fiduciary and informational-authority doctrine; Originating Informational Purpose; Purpose and Question Particularity; Authorization Friction; Authority-Capability Correspondence and Authority-Capability Delta; Government Population Golden Record and Functional Universal Search risks; identity and digital-service architecture; algorithmic and agentic systems; Relational Information; cybersecurity and abuse-detection processing; intergovernmental and cross-sovereign exchange; Independent Information Intermediaries and commercial information markets; public records, archives, preservation, and transparency; Vendor and shared-service capability; emergency and Exception Envelope practice; legacy remediation; learned computational artifacts; individual rights and remedies; conformance consistency; circumvention mechanisms; and constitutional or statutory developments; Positive Legal Authority / Legitimate Informational Authority separation; Purpose Divergence and Informational Justification Level determinacy; Necessary Standing Informational Capability; Structural Least Power; unnecessary or dormant standing capability; and implementation experience under T-70, CF-79, and SD-13.

#### **(c) Real-World Reference Testing**

The coordinated review shall include adversarial evaluation against representative governmental functions, including integrated benefits administration; state or local law enforcement; statewide fraud and program-integrity analytics; artificial intelligence agents and automated decision systems; cybersecurity and insider-abuse detection; emergency or break-glass access; multi-

Vendor and shared-service architectures; Independent Information Intermediary acquisition; and intergovernmental information exchange.

**(d) FCGIAS and Traceability Review**

The DTA shall review whether binding Trilogy Conformance Code provisions remain traceable to enacted authority; whether any incorporated technical control has become obsolete, overbroad, underprotective, or unsupported; whether new FCGIAS material should be incorporated through lawful rulemaking; and whether any substantive FCGIAS proposition requires legislative rather than regulatory action. The review shall include the current public Normative Traceability Matrix.

**(e) Public Participation**

The DTA shall provide meaningful opportunity for participation by affected individuals; civil-rights, civil-liberties, and privacy organizations; disability and accessibility advocates; state and local agencies; prosecutors and law-enforcement representatives; benefits and regulatory administrators; cybersecurity professionals; enterprise architects; technologists and identity experts; academics; Vendors; procurement officials; archivists and records officials; and other materially affected stakeholders.

**(f) No Automatic Sunset**

PDTA, VIDA, and GAAFA do not expire merely because a periodic review is required. Any repeal, suspension, or substantive expiration must be enacted by the Legislature.

## **Section 27. Severability**

**(a) General Severability**

If any provision of this Act, or the application of a provision to any person, governmental function, system, informational act, or circumstance, is held invalid or unenforceable, the invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application. To that end, the provisions of this Act are severable.

**(b) Fiduciary and Architectural Independence**

In particular:

- (1) invalidation of a constitutional finding does not invalidate an independently established statutory fiduciary duty;
- (2) invalidation of a particular architectural requirement does not invalidate the underlying duties of loyalty, care, confidentiality, or transparency and accountability;
- (3) invalidation of a private damages remedy does not invalidate declaratory, injunctive, administrative, or other remedies to the extent independently lawful;
- (4) invalidation of an application to one governmental function does not invalidate application to other governmental functions; and
- (5) invalidation of a provision applicable to government does not necessarily invalidate a provision applicable to vendors or other Secondary Information Fiduciaries, or vice versa.

**(c) Constitutional Avoidance**

Where a provision reasonably admits of more than one construction, a court shall prefer a construction that preserves the provision's validity while remaining faithful to its text and the purposes stated in Section 2.

## Section 28. Effective Date and Implementation

### (a) Effective Date

#### (a-1) Trilogy Transition Spine

This section supplies the generally applicable structural-transition, legacy-remediation, and safe-harbor framework for PDTA, VIDA, and GAAFA. VIDA and GAAFA may specify specialized inventory, classification, or remediation content for identity or Algorithmic Systems but shall not create a conflicting general transition period, safe harbor, or source of Governmental Informational Authority. Where a downstream Act states a more protective or earlier substantive compliance date for a specialized function, that date governs the specialized requirement.

Except as otherwise provided in this section, this Act shall take effect [180] days after enactment.

### (b) Immediate Organizational Authority

Upon enactment, the State may immediately undertake establishment and staffing of the DTA; rulemaking; development of FCGIAS implementation materials; inventories and conformance assessments; procurement revisions; training; technical assistance; grant administration; and planning necessary for implementation.

### (c) Transactional Obligations

Beginning on the general effective date, all Government Agencies and Secondary Information Fiduciaries shall comply with the transactional and fiduciary requirements of this Act, including prohibitions against unauthorized access; unauthorized disclosure; unauthorized secondary use; deliberate purpose laundering; retaliation; knowing concealment; unauthorized acquisition from an Independent Information Intermediary; and other informational acts capable of immediate compliance.

A legacy-system transition period does not create Governmental Informational Authority.

### (d) New Systems and New Structural Capability

Beginning on the general effective date, a Government Agency shall not newly construct, procure, activate, or materially expand a Government Population Golden Record; Functional Universal Search; standing cross-purpose AI access; unbounded administrative access; a Government-Intermediary Reacquisition Architecture; materially generalized intergovernmental search; Authorization-Free Material Expansion capability; or another Per Se Disloyal structural capability.

### (e) Existing Structural Nonconformance

A Government Agency operating a preexisting system that cannot achieve full structural conformance by the general effective date may receive a temporary Legacy Structural Remediation Safe Harbor only as provided by this section.

### (f) Conditions of Safe Harbor

The safe harbor applies only where the Government Agency:

- (1) identifies the nonconforming capability to the DTA within [12 months] after enactment;
- (2) identifies the Positive Legal Authority, Legitimate Informational Authority, and Necessary Standing Informational Capability supporting continued lawful functions;
- (3) ceases any use for which sufficient authority does not exist;

- (4) implements immediate least-power containment of the disclosed nonconforming capability to the maximum reasonably feasible extent, including, as applicable, disabling unnecessary universal or cross-purpose search or query paths; preventing addition of new information domains or materially new uses; restricting administrative and Vendor access; preventing capability expansion; imposing heightened logging and periodic review; and implementing technical or architectural restrictions where reasonably feasible. Policy instruction alone is insufficient where a materially effective technical containment measure is reasonably available;
- (5) submits a remediation plan;
- (6) establishes measurable remediation milestones;
- (7) submits to DTA review;
- (8) does not materially expand the nonconforming capability;
- (9) complies with all transactional requirements capable of immediate compliance; and
- (10) completes remediation within the period approved under subsection (g).

The DTA may deny, condition, suspend, or terminate the safe harbor where materially effective containment is reasonably feasible but is not implemented or maintained.

#### **(g) Duration**

A Legacy Structural Remediation Safe Harbor may remain in effect for no more than [48 months] after enactment unless the Legislature authorizes a longer period for a specifically identified class of systems. The DTA may establish shorter deadlines based upon risk, capability, feasibility, and governmental function.

#### **(h) Effect of Safe Harbor**

A valid safe harbor:

- (1) temporarily limits structural enforcement requiring immediate replacement or shutdown of the disclosed legacy capability;
- (2) does not declare the architecture substantively conforming;
- (3) does not create or enlarge Governmental Informational Authority;
- (4) does not immunize unauthorized informational acts;
- (5) does not immunize deliberate purpose laundering, retaliation, concealment, unauthorized disclosure, or knowing misuse;
- (6) does not prevent emergency judicial relief for an informational act causing imminent unlawful harm; and
- (7) terminates upon material violation of the approved remediation plan.

#### **(i) Existing Contracts**

Material existing contracts shall be brought into compliance at the earlier of renewal; material modification; [36 months] after enactment; or a shorter period ordered by the DTA where the arrangement presents substantial generalized informational risk.

#### **(j) Completion**

Upon expiration of the applicable transition period, all covered systems shall comply with the structural requirements of this Act and binding conformance regulations unless the Legislature expressly provides otherwise. Implementation delay shall not be construed as legislative approval of nonconforming architecture.

## Appendix A. Section-Level FCGIAS Version 2.2 Traceability

This appendix preserves the section-level traceability inherited from the FCGIAS Version 2.1 baseline and applies the controlling Version 2.2 legitimacy layer and adopted IR-01 Structural Least-Power clarification. The references are explanatory and do not incorporate nonstatutory FCGIAS material as substantive law except through regulations adopted under Section 25. Current conformance shall use FCGIAS Version 2.2, including T-61 through T-70, CF-70 through CF-79, and SD-12 through SD-13 where applicable.

### Version 2.2 Supplemental Traceability

T-61 through T-63: Positive Legal Authority, Legitimate Informational Authority, and Citizen-Originated Purpose → Sections 3, 6, 8, 9, 19, 20, 24, 25, and 28.

T-64 through T-66: Purpose Divergence, Informational Justification Levels, and Anti-Abstraction → Sections 3, 6, 8, 9, 20, 24, and 25.

T-67 through T-69: Positive-Authority Bootstrap, relational multi-person legitimacy, and conformance-legality separation → Sections 9, 14, 17, 20, 24, and 25.

T-70 / CF-79 / SD-13: Necessary Standing Informational Capability and Structural Least Power → Sections 3, 6, 14, 19, 20, 26, and 28.

| PDTA § | Section                                       | Principal FCGIAS 2.1 Trace               | Legislative Function                                                                                                               |
|--------|-----------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 1      | Short Title                                   | F-1; FCGIAS §§1-3                        | Identifies the statutory legal layer implementing ordered informational authority.                                                 |
| 2      | Findings and Purposes                         | F-1-F-10; FCGIAS §§3, 16-21, 124-128     | States limited authority, anti-general-power, fiduciary, capability, and doctrinal-calibration foundations.                        |
| 3      | Definitions                                   | FCGIAS §§24-27, 31-43, 65, 73-78         | Translates OIA, capability, ontology, discovery, intermediation, and trusteeship concepts into statutory terms.                    |
| 4      | Primary Information Trusteeship               | F-7; FCGIAS §§37, 73-74                  | Implements the primary informational relationship without relying on ownership or an express trust.                                |
| 5      | Government as Secondary Information Fiduciary | F-6, F-9; FCGIAS §§60-64                 | Makes governmental informational power fiduciary and separates authority from possession, capability, and commercial availability. |
| 6      | OIP and Governmental Informational Authority  | OIA-3-OIA-7; ACCP; FCGIAS §§22-25, 28-33 | Establishes OIP, Authorized Object,                                                                                                |

|    |                                                          |                                                 |                                                                                                                                                               |
|----|----------------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                                          |                                                 | authority-source requirements, capability limits, and ACCP.                                                                                                   |
| 7  | Fiduciary Duties                                         | FCGIAS §§60-63                                  | Codifies loyalty, care, confidentiality, and transparency/accountability.                                                                                     |
| 8  | Authorized Informational Acts and Material Expansion     | OIA-2, OIA-7; FCGIAS §§28-30, 38                | Separates informational operations and requires renewed authorization for Material Expansion.                                                                 |
| 9  | Purpose and Question Particularity                       | OIA-6, OIA-22; FCGIAS §§26-27                   | Defines particularity and bars purpose laundering while permitting unknown answers.                                                                           |
| 10 | Purpose Sequestration, Correlation, Inference, and Reuse | OIA-8-OIA-15, OIA-21; FCGIAS §§34-41, 59        | Implements functional sequestration, inherent processing, governed correlation/inference, reuse, and verification preference.                                 |
| 11 | Bounded Government Discovery                             | OIA-10-OIA-11, OIA-23; FCGIAS §§42-44           | Permits predicate-bounded, hypothesis-generating, and statistical discovery while prohibiting generalized discovery.                                          |
| 12 | Independent Information Intermediation                   | OIA-28-OIA-29; FCGIAS §§64-72                   | Implements III classification, asymmetric disclosure/acquisition rules, commercial-availability rule, transformation rule, and anti-reacquisition.            |
| 13 | Presumptively Disloyal Practices                         | FCGIAS §§40-44, 64-72; CF-14-CF-18, CF-63-CF-69 | Creates rebuttable fiduciary presumptions for high-risk informational acts while preserving lawful bounded uses.                                              |
| 14 | Per Se Disloyal Practices                                | FCGIAS §§36, 89-98; SD-1-SD-11                  | Makes structural generalized capability, Golden Records, universal search, policy-only controls, laundering, and related architecture categorically disloyal. |
| 15 | Rights of Primary Information Trustees                   | FCGIAS §§45-48, 60-63, 87                       | Implements notice, access, correction, derived-information correction, revocation, portability, explanation, and contestability.                              |
| 16 | Authorized Information                                   | FCGIAS §§73-74                                  | Implements bounded                                                                                                                                            |

|    |                                                                 |                                                  |                                                                                                                                          |
|----|-----------------------------------------------------------------|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
|    | Trustees and Guardianship                                       |                                                  | delegation and anti-recentralization while preserving PIT status.                                                                        |
| 17 | Government, Vendor, Agent, and Intergovernmental Responsibility | FCGIAS §§45, 79-81, 93-95                        | Prevents vendor, AI, and intergovernmental capability laundering and makes authority limits flow through delegated performance.          |
| 18 | Access, Processing, Retention, Preservation, and Recovery       | FCGIAS §§32, 84-88                               | Separates legal authorities for use, retention, preservation, public records, and recovery; expired authority is not restored with data. |
| 19 | Architectural and Conformance Obligations                       | FCGIAS §§31-36, 82-93, 96-111                    | States statutory structural outcomes while leaving detailed assessment methodology to binding conformance regulation.                    |
| 20 | Burdens of Proof and Evidentiary Rules                          | FCGIAS §§96-111; normative traceability doctrine | Allocates proof according to informational asymmetry and makes structural capability independently reviewable.                           |
| 21 | Private Right of Action                                         | FCGIAS §§96-111; enforcement layer               | Makes substantive fiduciary, authority, rights, and structural obligations judicially enforceable.                                       |
| 22 | Remedies                                                        | FCGIAS §§111-112                                 | Implements structural remedies and the Least-Power Remediation hierarchy.                                                                |
| 23 | Data Trusteeship Authority and Enforcement                      | FCGIAS §§96-112, 130-132                         | Creates the principal trilogy oversight institution for conformance, enforcement, and technical review.                                  |
| 24 | Relationship to VIDA, GAAFA, and Other Law                      | FCGIAS §§120-124, 130                            | Maintains PDTA as legal layer, VIDA as identity/architecture layer, and GAAFA as AI/decisional layer under one authority model.          |
| 25 | Rulemaking and FCGIAS Conformance                               | FCGIAS §§96-106, 120-123, 129-132                | Makes FCGIAS a technical reference downstream from law and preserves legislative control over substantive rights and authority.          |

|    |                                   |                               |                                                                                                                                  |
|----|-----------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 26 | Periodic Review                   | FCGIAS §§113-119, 129         | Requires recurring adversarial testing against real governmental use cases and technological change.                             |
| 27 | Severability                      | FCGIAS §124; D1-D4 separation | Preserves statutory fiduciary architecture independently from contested constitutional propositions or particular remedies.      |
| 28 | Effective Date and Implementation | FCGIAS §§96-112, 129          | Separates immediate transactional duties from staged legacy structural remediation without granting new informational authority. |

#### Appendix Note: Normative Priority

The traceability chain is:

*FOUNDATIONAL PRINCIPLE → ORDERED INFORMATIONAL AUTHORITY RULE → ARCHITECTURAL INVARIANT → STATUTORY DUTY OR PROHIBITION → BINDING TECHNICAL STANDARD OR CONTROL → CONFORMANCE TEST → ENFORCEMENT OR REMEDY.*

Where a conflict exists, the Constitution and enacted law control. FCGIAS and implementing regulations may operationalize the statute but may not independently enlarge Governmental Informational Authority or diminish substantive statutory protections.