

GOVERNMENT ALGORITHMIC ACCOUNTABILITY AND AI FIDUCIARY ACT

Version 2.2 Clean Restated Legislative Candidate

Prepared by Michael G. Leahy
September 13, 2026

An Act to govern governmental use of artificial intelligence, automated decision systems, algorithmic analytics, agentic systems, and computational inference; to preserve accountable governmental decision-making; to require authority-bounded deployment, meaningful decisional explanation, contestability, provenance, testing, and human judgment where legally material; to regulate population-scale governmental analytics without converting scale into generalized informational power; and to implement the Personal Data Trusteeship Act, the Verifiable Identity and Digital Autonomy Act, and the Fiduciary Commons Government Information Architecture Standard.

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

SECTION 1. SHORT TITLE

(a) This Act may be cited as the “Government Algorithmic Accountability and AI Fiduciary Act” or “GAAFA.”

SECTION 2. LEGISLATIVE FINDINGS, PURPOSES, AND GOVERNING PRINCIPLE

(a) Findings

(1) Artificial intelligence and automated computational systems increasingly make, recommend, rank, score, prioritize, predict, classify, retrieve, correlate, infer, or otherwise materially influence governmental action.

(2) The legal significance of governmental AI arises from the governmental informational and decisional capability exercised through the system, not from whether the technology is labeled artificial intelligence.

(3) Artificial intelligence may increase government’s capacity to execute lawful authority but does not enlarge that authority.

(4) A governmental system may be technically accurate yet unlawful if it obtains, correlates, infers from, or acts upon information beyond the authority supporting the governmental function.

(5) A system may be technologically opaque without necessarily being unlawful if government can establish the legally and factually material basis for an affected decision, while a nominally interpretable model may remain unlawful if its use, inputs, inferences, or consequences exceed governmental authority.

(6) Persons affected by material governmental decisions require meaningful notice, explanation, correction, contestability, and review sufficient to test the lawful and factual basis of the decision.

(7) Human involvement does not provide meaningful accountability when the official lacks legal authority, relevant information, practical ability to disagree, adequate time, or institutional freedom to exercise independent judgment.

(8) Population-scale analytics may serve legitimate governmental purposes, including fraud detection, program integrity, public health, cybersecurity, resource planning, and discovery, but scale does not create generalized authority to search for unspecified patterns or individualized knowledge.

(9) Algorithmic inference can create new individualized informational artifacts that government did not previously possess; technical ability to infer does not create authority to infer.

(10) Commercially generated scores, profiles, predictions, classifications, or model outputs do not become authorized governmental knowledge merely because a private entity lawfully generated or possessed them.

(11) Agentic and composite automated systems may execute multi-step governmental functions, but software is not thereby a legal fiduciary or independent source of governmental authority; accountable natural persons and legal entities remain responsible.

(12) Durable governance should regulate actual capability, authority, consequence, provenance, and accountability rather than mandate or prohibit particular model families merely by technical label.

(13) Positive Legal Authority is a necessary source of governmental power but does not, by itself, establish that every computational or informational capability authorized in the abstract is legitimate or necessary as ordinary standing capability.

(14) Legitimate Informational Authority establishes an outer ceiling on governmental informational power; ordinary standing technical capability should be narrower where a materially less informationally powerful architecture can reasonably perform the legitimate standing function.

(15) Predictive utility, administrative convenience, commercial availability, or broad program authorization does not independently justify Purpose Divergence, Material Derived Inference, generalized population analytics, or unnecessary standing capability.

(b) Purposes

(1) implement PDTA's Ordered Informational Authority, Legitimate Informational Authority, and Authority-Capability Correspondence requirements at the computational and decisional layer;

(2) require predeployment assessment of governmental authority, informational operations, model materiality, and decisional consequences;

(3) classify governmental AI according to actual function and consequence rather than vendor characterization;

(4) preserve meaningful governmental accountability for material decisions;

(5) establish meaningful decisional explanation, notice, correction, contestability, and review;

(6) distinguish lawful bounded analytics from generalized informational power;

(7) govern Material Derived Inference, Material Secondary Correlation, Bounded Government Discovery, and population-scale analytics;

(8) prevent vendors, commercial information intermediaries, governmental partners, and automated systems from laundering informational or decisional capability;

(9) require lifecycle testing, monitoring, provenance, civil-rights review, change management, and remediation; and

(10) preserve technology neutrality while establishing architecture-specific and consequence-specific legal requirements; and

(11) cause Standing Technical Informational Capability to correspond to, and not materially exceed, Necessary Standing Informational Capability, which in turn SHALL remain within Standing Legitimate Informational Authority.

(c) Governing Principle

Artificial intelligence may exercise governmental informational and decisional capability only within the purpose, authority, informational boundaries, and permitted consequences that would govern the governmental function if performed without artificial intelligence. Positive Legal Authority is necessary where applicable but is not self-validating as to the legitimacy or necessity of every standing capability. Standing Technical Informational Capability SHALL correspond to, and SHALL NOT materially exceed, Necessary Standing Informational Capability, which SHALL remain within Standing Legitimate Informational Authority. AI may increase government's capacity to execute lawful authority; it does not enlarge that authority.

SECTION 3. DEFINITIONS

(a-1) Trilogy Definition Inheritance

Capitalized terms defined by PDTA or, where applicable to an identity operation, VIDA have the meanings established by those Acts unless this Act expressly defines a specialized algorithmic or automated-system term. A specialized definition does not create Governmental Informational Authority by implication.

(a) The following specialized definitions apply to algorithmic, automated-system, and AI functions. They supplement PDTA and, where applicable to identity operations, VIDA and do not create Governmental Informational Authority by implication.

(b) Definitions

"Accountable Human Official" means an identified government officer or employee who possesses lawful authority over the relevant governmental action and, where this Act requires Meaningful Human Judgment, satisfies Section 14.

"Agentic System" means an automated system capable of pursuing goals, selecting or sequencing actions, invoking tools or services, querying or processing information, or producing external effects without explicit human direction for each individual step.

"Algorithmic Authority and Deployment Assessment" or "AADA" means the predeployment assessment required by Section 9.

"Algorithmic Impact Assessment" or "AIA" means the lifecycle evaluation required by Section 26.

"Algorithmic System" means software, a model, algorithm, statistical process, rules engine, machine-learning system, large language model, agentic system, or other computational process that materially performs an informational, analytical, or decisional governmental function.

"Analytics-Adjudication Separation" means the structural and procedural separation required by Section 23 between hypothesis-generating analytics and an individualized adverse governmental consequence.

"Composite Machine Action" means an outcome produced through a sequence or combination of models, agents, tools, retrieval systems, rules, databases, or automated services where no single component alone represents the complete governmental action.

"Derived Information" means information, classification, score, prediction, estimate, inference, relationship, ranking, or other informational artifact produced through processing rather than directly observed or supplied as an established fact.

"Epistemic Status" means the documented status of an informational artifact as observed, reported, verified, inferred, predicted, estimated, disputed, corrected, stale, or otherwise qualified.

"Feature" means an input, variable, representation, embedding, proxy, transformed value, or other informational element materially used by an Algorithmic System.

"Material Governmental Decision" means a governmental determination, recommendation, prioritization, ranking, score, classification, referral, enforcement action, benefit or service determination, license or permit action, legal-status determination, or other action that materially affects a person's rights, duties, benefits, liberties, opportunities, legal status, access to government, or exposure to governmental investigation or enforcement.

"Meaningful Decisional Explanation" means the case-specific explanation required by Section 15.

"Meaningful Human Judgment" means independent human governmental judgment satisfying Section 14.

"Model Materiality" means the degree to which an Algorithmic System's output changes, constrains, structures, prioritizes, or practically determines a governmental action or the information available to the official making it.

"Purpose-Bounded Analytics Enclave" means a computational environment in which authorized data, operations, users, models, outputs, retention, and export are bounded to a sufficiently particular governmental analytical purpose.

"Question Particularity" has the meaning established by PDTA.

"Signal" means an analytical output indicating a pattern, anomaly, risk, association, or hypothesis that has not yet been established as an adjudicative fact.

"Tier I System" means a Material Governmental Decision System under Section 7.

"Tier II System" means a Governmental Analytical System under Section 7.

"Tier III System" means an Assistive or Ministerial System under Section 7.

"Vendor" has the meaning established by PDTA.

SECTION 4. RELATIONSHIP TO PDTA, VIDA, AND FCGIAS

(a) PDTA governs Governmental Informational Authority, fiduciary duties, rights, structural limitations, enforcement, and remedies. VIDA governs identity and digital-service architecture. This Act governs computational, analytical, algorithmic, automated, and AI-mediated exercise of governmental informational and decisional capability.

(b) FCGIAS provides the technical and conformance framework to the extent incorporated through PDTA and binding DTA regulation.

(c) Nothing in this Act creates governmental authority to collect, access, query, compare, correlate, infer, disclose, retain, identify, resolve, rank, score, classify, predict, or act upon information.

(d) Where an Algorithmic System performs an identity operation governed by VIDA, both Acts apply to their respective functions.

(e) An automated system is not a legal Secondary Information Fiduciary solely by reason of being software. The Government Agency, Governmental Actor, Vendor, or other legally cognizable entity remains accountable under applicable law.

(f) Common Trilogy Machinery

PDTA provisions governing Composite Governmental Information Transactions, Responsible Government Agencies, Role Stacking, Exception Envelopes, the Trilogy Conformance Code, Vendor responsibility, burdens, remedies, and transition apply to systems governed by this Act except where this Act expressly supplies a more specific algorithmic or decisional rule.

SECTION 5. AI BOUNDARY INHERITANCE AND INSTITUTIONAL ACCOUNTABILITY

(a) Every Algorithmic System SHALL inherit the Originating Informational Purpose, Positive Legal Authority, Legitimate Informational Authority, jurisdiction, informational-domain, operation, predicate, duration, disclosure, retention, permitted-consequence, and Purpose-Divergence boundaries applicable to the governmental function it serves.

(b) A system SHALL NOT obtain or construct information that the governmental actor or function would lack authority to obtain or construct merely because automated processing makes the operation possible.

(c) Government remains responsible for capability exercised through Vendors, agents, models, APIs, hosted services, commercial products, or governmental partners.

(d) No agency may defend a violation by asserting that a model independently selected the information, inference, action, tool, or consequence.

(e) Material limitations SHALL, where reasonably feasible, be enforced structurally rather than principally through operator instruction.

(f) Structural Least Power. Before government deploys or maintains a material standing algorithmic capability, it SHALL determine whether a materially less informationally powerful architecture can reasonably perform the legitimate standing function. Broader capability MAY become available only when the governmental relationship, predicate, purpose, authority, and necessity have expanded sufficiently to justify it.

SECTION 6. GOVERNMENTAL INFORMATIONAL OPERATIONS

(a) An AADA SHALL identify each material informational operation performed by the system, including READ, QUERY, COMPARE, CORRELATE, INFER, CLASSIFY, RANK, SCORE, PREDICT, DISCLOSE, EXPORT, RETAIN, IDENTIFY, RESOLVE, or ACT UPON INFORMATION.

(b) Authority for one informational operation does not imply authority for another.

(c) Inherent processing logically necessary to execute an already authorized governmental function may occur without a separate authorization event, but Material Secondary Correlation or Material Derived Inference requires authority sufficient for that operation.

(d) Material expansion of scope, persons, domains, inferential power, permitted consequence, or reusable standing capability requires Materially Renewed Authorization that is both legally sufficient and substantively sufficient under PDTA.

SECTION 7. SYSTEM CLASSIFICATION BY ACTUAL USE AND CONSEQUENCE

(a) Tier I - Material Governmental Decision Systems A system is Tier I when, in actual governmental use, it makes, recommends, ranks, scores, prioritizes, refers, or otherwise has a material practical effect on a Material Governmental Decision. Material influence is determined from the system's actual workflow effect, including whether its output materially changes the probability, timing, intensity, burden, or outcome of governmental review or action.

(b) Tier II - Governmental Analytical Systems A system is Tier II when it performs discovery, analytics, forecasting, resource planning, fraud detection, pattern identification, risk analysis,

cybersecurity analysis, public-health analysis, or similar functions and its output does not itself materially determine, trigger, prioritize, or intensify an individualized adverse governmental consequence. A nominally analytical system used in a manner meeting subsection (a) is Tier I for that use.

(c) Tier III - Assistive and Ministerial Systems A system is Tier III when it performs drafting, summarization, translation, retrieval, routing, scheduling, citizen navigation, or similar assistance and neither materially determines governmental treatment nor independently expands Governmental Informational Authority.

(d) Classification turns on actual capability, use, workflow, and consequence, not product label.

(e) A system operating in more than one tier SHALL satisfy the requirements applicable to each use, and the highest applicable safeguards govern the material operation at issue.

(f) Material drift into a higher tier requires reclassification and any required predeployment approval before the higher-tier use begins.

SECTION 8. TIER-SPECIFIC BASELINE REQUIREMENTS

(a) Tier I systems are subject to the full AADA, Meaningful Human Judgment where required, Meaningful Decisional Explanation, notice, contestability, correction, provenance, lifecycle AIA, civil-rights testing, and DTA conformance requirements.

(b) Tier II systems are subject to an AADA proportionate to risk, Question Particularity, Bounded Government Discovery where applicable, provenance, output controls, Analytics-Adjudication Separation, lifecycle testing, and change management.

(c) Tier III systems are subject to purpose and authority limits, source and accuracy controls appropriate to use, disclosure where a person reasonably could mistake the system for a human or authoritative final decision-maker, human escalation where necessary, and drift prevention.

(d) The DTA may establish proportionate documentation requirements by regulation but may not exempt a system from substantive statutory requirements applicable to its actual use.

(e) Emergency or exigent governmental use does not create new authority. Where delay required to complete ordinary predeployment documentation would materially threaten life, safety, cybersecurity, continuity of essential government, or another independently recognized exigency, an agency may temporarily deploy a system within existing legal authority if it documents the trigger, scope, accountable official, permitted operations, duration, and post-use review; completes the otherwise required AADA as soon as reasonably practicable; and terminates or narrows the exceptional capability when the exigency ends.

(f) Exception Envelope

Emergency, exigent, temporary, or exceptional algorithmic capability SHALL be implemented within the PDTA Exception Envelope, including PDTA's invocation-specific activation and immediate-emergency rules. The envelope SHALL identify the system, authorized tools and data, permitted operations and outputs, accountable official, duration, audit, termination, and any required retrospective AADA, notice, correction, or remediation. The envelope does not supply missing Governmental Informational Authority and does not create standing algorithmic permission merely because it has been preapproved.

SECTION 9. ALGORITHMIC AUTHORITY AND DEPLOYMENT ASSESSMENT

(a) Before deploying a new Tier I system or a material Tier II system, a Government Agency SHALL complete and approve an AADA through the accountable agency official designated by law or regulation. The agency SHALL file the AADA or required summary with the DTA as prescribed by regulation. DTA predeployment approval is required only for categories expressly identified by this Act or by a risk-based regulation promulgated under Section 36 pursuant to intelligible statutory criteria including consequence, scale, novelty, irreversibility, use of sensitive information, or material Authority-Capability Delta.

(b) Required contents

- (1) governmental function, Originating Informational Purpose, and any material Purpose Divergence;
- (2) Positive Legal Authority supporting each material informational and decisional operation, together with the Legitimate Informational Authority claimed for the deployment;
- (3) Authorized Objects, populations, information domains, and permitted consequences;
- (4) system description, architecture, interfaces, tools, models, and external dependencies;
- (5) Standing Legitimate Informational Authority, Necessary Standing Informational Capability, Standing Technical Informational Capability, and Authority-Capability Delta;
- (6) features, material inputs, correlations, inferences, outputs, and Model Materiality;
- (7) training, fine-tuning, grounding, retrieval, validation, and testing sources to the extent material and available;
- (8) provenance and Epistemic Status controls;
- (9) accuracy, reliability, known limitations, false-positive and false-negative consequences where measurable and relevant;
- (10) civil-rights and disparate-outcome testing appropriate to the function;
- (11) adversarial and negative-capability testing;
- (12) human judgment and contestability architecture;
- (13) Vendor, Independent Information Intermediary, and commercial-data involvement;
- (14) retention, logging, audit, security, and change-management controls;
- (15) PDTA, VIDA, GAAFA, and FCGIAS conformance; and
- (16) Informational Justification Level, Authorized Answer opportunities, Least Informational Power analysis, and alternatives considered that would create materially less governmental informational or decisional power while reasonably performing the legitimate function.

(c) A materially changed deployment requires an updated AADA before the change is used where the change materially affects authority, data, features, model behavior, population, consequence, or ACD.

(d) Public disclosure of an AADA is governed by Section 37 and applicable public-records law. Security-sensitive, privileged, procurement-sensitive, confidential-source, law-enforcement-sensitive, and trade-secret information may be withheld only to the extent independently authorized by law; such protection does not limit DTA access where the DTA is legally authorized to receive the information and maintains required safeguards.

SECTION 10. PURPOSE AND QUESTION PARTICULARITY

(a) Question Particularity has the meaning established by PDTA. For an Algorithmic System, application of that standard SHALL identify, at minimum, the governmental question, Originating Informational Purpose, relevant information domains, authorized computational operations, expected outputs, prohibited uses, permitted governmental consequences, Purpose Divergence, and the boundary beyond which Materially Renewed Authorization is required. The analytical question SHALL remain within Legitimate Informational Authority even where a governmental program possesses broad Positive Legal Authority.

(b) Phrases such as "government efficiency," "public safety," "program integrity," "fraud," "analytics," "innovation," or "citizen services" are insufficient standing alone and SHALL NOT be used to abstract a materially broader informational purpose from the particular governmental function.

(c) Uncertainty about which person, event, transaction, or pattern will be discovered does not defeat particularity if the governmental question, domains, operations, scope, and permitted consequence are sufficiently bounded.

(d) A materially different analytical question requires renewed authority where required by PDTA.

SECTION 11. FEATURE, MODEL, TRAINING, GROUNDING, AND PROVENANCE AUTHORITY

(a) Every material information domain and Feature family used by a Tier I or material Tier II system SHALL be supported by Positive Legal Authority where required and by Legitimate Informational Authority appropriate to the model's particular purpose, operation, consequence, and Informational Justification Level, or be a lawful transformation of information satisfying those requirements.

(b) A Feature does not become legitimate or authorized merely because it is statistically predictive, operationally useful, commercially available, or technically accessible.

(c) Training Data, fine-tuning data, retrieval corpora, grounding sources, embeddings, external tools, and model context SHALL be evaluated according to the governmental use made of them and the informational capability they create.

(d) Government SHALL maintain provenance sufficient to identify material sources and transformations relied upon for Tier I decisions and material Tier II signals, subject to lawful security protections.

(e) Where a Vendor cannot provide material provenance necessary for lawful governmental use, government SHALL not use the system for that function unless an independently sufficient validation method supplies equivalent accountability.

(f) Government-Purpose Training and Adaptation

Government or a bounded Vendor may train, fine-tune, adapt, configure, ground, index, embed, retrieve against, or otherwise improve an Algorithmic System for a governmental purpose only to the extent Positive Legal Authority and Legitimate Informational Authority support the information and operation involved; the use is sufficiently particular and reasonably necessary; Purpose Sequestration is preserved; independent Vendor or commercial reuse is not thereby authorized; and the resulting informational capability remains within the legitimate governmental function. Combining information from more than one governmental purpose does not merge those purposes or authorities and does not by itself authorize deployment or reuse of the resulting model or artifact for another governmental purpose.

(g) Learned and Derived Computational Artifacts

Model weights, embeddings, vector stores, feature stores, retrieval indexes, learned representations, fine-tuned adapters, persistent prompts or instruction sets containing material governmental information, and comparable computational artifacts SHALL be classified and governed according to the informational and inferential capability they materially preserve or create. Such an artifact does not become noninformational merely because its contents are mathematically encoded, statistically distributed, compressed, or impracticable to interpret record-by-record.

(h) Artifact Capability Assessment

For a material Tier I or Tier II deployment, the AADA SHALL identify learned or derived computational artifacts that materially permit retrieval, association, reconstruction, classification, inference, or individualized action; the authority supporting their creation and use; retention and deletion conditions; portability or Vendor custody where relevant; and whether continued possession of the artifact would preserve Standing Technical Capability after the underlying authority expires.

(i) Learned-Artifact Expiration, Divergent Reuse, and Reconstitution

When authority supporting a learned or derived computational artifact expires or materially contracts, or when government proposes to retain or reuse the artifact for a materially divergent purpose, the Government Agency SHALL apply PDTA requirements governing Purpose Divergence, Materially Renewed Authorization, learned-artifact expiration, and reconstitution. 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 information authorized and legitimate for the new use before further operational use. Lawful preservation does not authorize operational reuse.

SECTION 12. VENDOR AND COMMERCIAL-SYSTEM PREDEPLOYMENT ASSESSMENT

(a) Government SHALL assess Vendor and commercial systems as governmental capability within the Assessment Boundary to the extent government can exercise that capability through ordinary contractual, technical, administrative, or operational arrangements. This conformance attribution does not itself make the Vendor a governmental fiduciary or establish constitutional state action.

(b) Contractual confidentiality, trade-secret claims, or proprietary architecture do not excuse the Government Agency from obtaining information sufficient to determine conformance and lawfully explain material governmental action.

(c) Government SHALL evaluate whether the Vendor can independently retain, aggregate, enrich, train upon, profile, sell, disclose, or reuse governmental information or derived outputs.

(d) Government SHALL NOT procure a system whose ordinary Standing Technical Informational Capability materially exceeds Necessary Standing Informational Capability merely because broader capability is positively authorized, commercially bundled, technically convenient, or potentially useful in another circumstance.

(e) Contracts SHALL require material change notice, regulator access, testing cooperation, purpose and use limits, subcontractor controls, security, retention, termination, and remedies appropriate to the deployment.

(f) A Vendor does not become a governmental fiduciary merely by contracting with government or providing governmental informational or decisional capability. Vendor duties arise from duties expressly imposed by PDTA, this Act, VIDA where applicable, procurement requirements,

contract, applicable agency principles, and other applicable law. Governmental fiduciary duties and informational-authority limits remain nondelegable.

SECTION 13. COMMERCIAL OUTPUTS AND INDEPENDENT INFORMATION INTERMEDIARIES

- (a)** Commercial availability does not create Governmental Informational Authority.
- (b)** A commercially generated score, classification, prediction, identity resolution, profile, inference, or model output is a governmental informational acquisition when government obtains or uses it and SHALL be assessed accordingly.
- (c)** The lawful possession or generation of information by an Independent Information Intermediary does not establish government's lawful authority to know or use it.
- (d)** Government SHALL NOT use a commercial output as a substitute for an independently sufficient governmental factual or legal basis where an individualized adverse consequence requires such a basis.
- (e)** Government SHALL assess reacquisition loops in which governmental information is disclosed to an intermediary, enriched or transformed, and later reacquired by government as a composite transaction under PDTA.

SECTION 14. MEANINGFUL HUMAN JUDGMENT

- (a)** Where law or this Act requires human judgment, the reviewing official SHALL possess lawful decisional authority, access to material evidence, sufficient understanding of the automated contribution, practical ability to disagree or modify the proposed action, adequate time, and institutional freedom to exercise independent judgment.
- (b)** Batch approval, rubber-stamping, nominal review, or review without material rationale does not constitute Meaningful Human Judgment.
- (c)** The official need not understand every mathematical parameter of a model but SHALL understand the system's material role, principal case-specific factors, known limitations relevant to the case, and the legal standard governing the decision.
- (d)** The record SHALL identify the accountable official and material disposition where human judgment is required.
- (e)** Pre-action individual human review is required only where applicable law requires human judgment or where the automated contribution creates a material risk that cannot reasonably be addressed through timely post-action review. The DTA may, by risk-based regulation, identify classes of ministerial or low-consequence Tier I actions for which post-action review is sufficient, and classes of high-consequence actions for which Meaningful Human Judgment is required, consistent with the statutory criteria in Sections 7 and 8.

SECTION 15. MEANINGFUL DECISIONAL EXPLANATION

- (a)** A person materially adversely affected by a Tier I system has the right to a Meaningful Decisional Explanation sufficient to understand and contest the governmental basis for the action, subject to independently applicable law governing security, privilege, confidential sources, investigations, protected personal information, and other lawful withholding.
- (b)** The explanation SHALL provide, to the extent material and reasonably available: the governmental decision; role of the Algorithmic System; principal case-specific factors; material data or classifications relied upon; relevant thresholds or rules; Epistemic Status of material

Derived Information; material known limitations; identity or office of the accountable reviewer where applicable; correction and contest pathways; and the governing legal or program criteria.

(c) The explanation need not disclose source code, every model weight, protected security information, or proprietary details unnecessary to test the decision's lawful and factual basis.

(d) If government cannot provide an explanation sufficient to permit meaningful contest of a material adverse decision, the agency SHALL not rely on the unexplained automated contribution as the sole material basis for sustaining the adverse action. The agency SHALL provide an independently reviewable basis sufficient under applicable law, conduct de novo review of the disputed contribution, or cease reliance on that contribution.

(e) The DTA may establish standardized explanation formats by regulation.

SECTION 16. NOTICE OF MATERIAL AUTOMATED INVOLVEMENT

(a) When a Tier I system materially influences an individualized adverse governmental action, the affected person SHALL receive notice of that material automated involvement at or before communication of the action unless delayed notice is independently authorized by law.

(b) Notice SHALL identify the governmental entity, general function of the system, nature of its material role, and available explanation, correction, and review rights.

(c) Notice requirements do not compel disclosure that would unlawfully compromise an investigation, security operation, protected source, or other legally protected interest; delayed or modified notice SHALL be no broader than necessary.

SECTION 17. CONTESTABILITY AND INDEPENDENT REVIEW

(a) A person materially adversely affected by a Tier I system SHALL have a meaningful opportunity to contest material factual errors, Derived Information, identity associations, classifications, and the application of governing criteria.

(b) Where the automated contribution is disputed and material, review SHALL be conducted by an official or body capable of exercising independent judgment and not bound by the challenged output.

(c) Review SHALL be de novo as to a disputed automated contribution when the affected person otherwise lacks a meaningful opportunity to test the material factual or inferential basis of the adverse action, unless another law establishes a different review standard sufficient to satisfy applicable procedural rights.

(d) Government SHALL preserve sufficient records to permit meaningful review while respecting PDTA's separate rules governing processing and preservation authority.

(e) Nothing in this section diminishes greater procedural rights otherwise provided by law.

SECTION 18. CORRECTION AND DERIVED INFORMATION CORRECTION

(a) Where a material input is corrected, government SHALL identify material Derived Information and downstream decisions reasonably likely to have been affected by the erroneous input.

(b) A person may contest a material Derived Information artifact and present evidence concerning its accuracy, context, provenance, or Epistemic Status.

(c) Government SHALL correct, qualify, suppress, or cease reliance upon Derived Information shown to be materially inaccurate, unlawfully generated, obsolete for the purpose, or unsupported at the level of confidence required for the consequence.

(d) Correction of source information SHALL not be deemed complete if a materially consequential derived score, classification, or inference continues to operate as though the erroneous source remained true.

SECTION 19. MATERIAL DERIVED INFERENCE

(a) Technical ability to infer does not create authority to infer.

(b) A Material Derived Inference concerning an identifiable person requires a sufficiently particular governmental purpose, Positive Legal Authority where required, Legitimate Informational Authority independently sufficient for the inference, authorized and justified inputs, documented provenance, and an Epistemic Status appropriate to the governmental consequence. Predictive utility does not itself establish legitimacy.

(b-1) Relational Information

Where an Algorithmic System creates, ranks, scores, predicts, resolves, or acts upon a relationship, network, household, association, transaction pattern, device association, event linkage, or other Relational Information, the resulting artifact and consequence remain subject to PDTA and this Act. Government SHALL NOT avoid provenance, Epistemic Status, correction, explanation, contestability, retention, Feature Authority, or conformance requirements by treating the output as relational rather than individualized. Where rights or assertions of multiple persons conflict, the system and responsible Government Agency SHALL apply PDTA Section 19's conflicting-relational-interests rule before treating a disputed relationship as authoritative for a material adverse consequence.

(c) An inference SHALL NOT be treated as an established fact merely because a model assigns high confidence to it.

(d) Where an adverse governmental consequence materially depends upon an inference, the agency SHALL establish the level of corroboration, verification, or evidentiary support required by applicable law and the consequence.

(e) Sensitive or constitutionally protected characteristics receive no categorical exemption from legitimate governmental use, but their inference requires authority and necessity sufficient for the specific governmental function and all applicable constitutional and civil-rights protections.

SECTION 20. BOUNDED GOVERNMENT DISCOVERY

(a) Government may use Algorithmic Systems to discover previously unknown persons, events, transactions, relationships, anomalies, or patterns where the discovery activity is supported by a sufficiently particular governmental purpose and authority.

(b) Bounded Government Discovery SHALL define the authorized question, information domains, operations, population or object scope where applicable, outputs, retention, escalation criteria, and permitted consequences.

(c) Discovery authority does not itself establish authority to impose an individualized adverse consequence.

(d) A discovered Signal may justify a separately authorized investigative or adjudicative step only where the applicable legal predicate is satisfied.

(e) Discovery SHALL NOT become a standing generalized search for unspecified wrongdoing or individualized knowledge. A Purpose-Generalized or IJ-4 population-scale capability is presumptively nonconforming unless a specific enacted authority expressly defines and bounds the capability and the deployment satisfies PDTA's substantive informational-justification and structural safeguards.

SECTION 21. PURPOSE-BOUNDED ANALYTICS ENCLAVES

(a) Material cross-domain Tier II analytics shall, where reasonably practicable, occur within a Purpose-Bounded Analytics Enclave or functionally equivalent architecture.

(b) The enclave SHALL restrict authorized data, users, models, operations, exports, retention, and reuse to the approved analytical purpose.

(c) Transient computational integration within an enclave does not itself violate Purpose Sequestration if the information cannot be converted into standing generalized access and outputs remain bounded.

(d) The enclave SHALL NOT become a permanent cross-purpose data lake, universal query service, reusable population profiling environment, or other standing capability materially broader than Necessary Standing Informational Capability.

SECTION 22. HYPOTHESIS-GENERATING ANALYTICS AND EPISTEMIC STATUS

(a) Governmental analytics may generate hypotheses, Signals, anomaly indicators, rankings, or risk estimates where authorized.

(b) A hypothesis-generating output SHALL be marked and treated according to its Epistemic Status and SHALL NOT silently become an established governmental fact.

(c) Systems and workflows SHALL preserve distinctions among observed facts, verified facts, allegations, inferred attributes, predictions, estimates, and disputed information.

(d) A Signal may be retained only for the period and purpose authorized under Section 24 and PDTA.

(e) Government SHALL establish escalation criteria separating analytical interest from investigative or adjudicative action.

SECTION 23. ANALYTICS-ADJUDICATION SEPARATION

(a) A Tier II Signal SHALL NOT by itself impose or automatically trigger an individualized adverse governmental consequence unless the system has been classified and governed as Tier I for that consequence.

(b) Before an adverse consequence based materially on a Tier II output, government SHALL establish the independently required legal and factual predicate through a process appropriate to the consequence.

(c) Where analytics merely prioritize lawful review, the agency SHALL assess whether prioritization itself materially affects rights, burdens, investigation exposure, or opportunity and therefore constitutes Tier I use.

(d) Government SHALL not avoid Tier I safeguards by labeling a materially determinative score or referral as advisory.

SECTION 24. SIGNAL RETENTION AND TRANSIENT COMPUTATIONAL INTEGRATION

(a) Signals, intermediate outputs, embeddings, temporary joins, and other computational artifacts SHALL be retained only as authorized and reasonably necessary for the approved purpose, validation, audit, contestability, security, or lawful preservation.

(a-1) Cybersecurity and Abuse-Detection Analytics

Algorithmic cybersecurity, insider-threat, account-abuse, service-integrity, and fraud-against-system analytics MAY operate across technical telemetry and otherwise sequestered domains

only within the PDTA cybersecurity and abuse-detection profile. The security profile concerns protection of systems, services, accounts, credentials, authentication or Technical Authorization mechanisms, confidentiality, integrity, availability, resilience, and technical misuse or compromise. A security Signal, anomaly score, relationship graph, or model output SHALL preserve provenance and Epistemic Status appropriate to its use and SHALL NOT be converted into an adverse programmatic, disciplinary, eligibility, regulatory, investigative, or law-enforcement consequence unless independently sufficient authority supports that materially different use, Materially Renewed Authorization is obtained where required, and applicable Tier I safeguards are satisfied. Discovery during security processing does not itself supply authority for the substantive use.

(b) Temporary cross-domain computation does not create continuing authority to retain the integrated dataset or reuse it for another purpose.

(c) Retention for validation, audit, or legal preservation does not imply continued authority for operational processing.

(d) Systems shall, where reasonably practicable, technically separate transient analytical state from durable operational records.

SECTION 25. MODEL MATERIALITY AND COMPOSITE MACHINE ACTION

(a) An agency SHALL assess Model Materiality according to the system's practical effect on governmental action, not merely whether a human formally makes the final decision.

(b) Composite Machine Action SHALL be assessed end-to-end. Government SHALL NOT fragment a workflow among multiple low-risk components to avoid requirements applicable to the resulting material governmental action.

(c) Where multiple models or agents collectively produce a Tier I consequence, provenance and accountability SHALL be sufficient to identify the material contribution of the composite workflow.

(d) A component that merely formats or transports an already lawful decision need not be treated as materially decisional solely because it uses AI.

(e) Composite Governmental Information Transaction

A multi-system or multi-entity AI workflow that constitutes a Composite Governmental Information Transaction under PDTA SHALL be assessed end-to-end for the separately applicable purposes and authorities, informational operations, Model Materiality, decision consequence, Vendor participation, authorization transitions, and aggregate Standing Technical Capability. No agency or Vendor may fragment a workflow to avoid classification or responsibility. Composite assessment does not merge the separate authority, predicate, jurisdiction, or permitted consequence of participating agencies, programs, or sovereigns.

(f) Responsible Government Agency

Where a composite deployment materially spans multiple Government Agencies, Vendors, models, agents, or shared services, the Responsible Government Agency required by PDTA SHALL maintain accountability sufficient to identify material responsibility for deployment approval, data and Feature authority, model behavior, consequential actions, and remediation. Other participants retain independent obligations for their conduct. RGA designation does not transfer or enlarge Governmental Informational Authority or programmatic decisional authority. Shared AI platforms may use layered responsibility consistent with PDTA.

(g) Role Stacking

A Vendor, Government Agency, operator, model provider, data provider, or other entity occupying more than one functional role is subject to the duties applicable to each role actually performed. A model provider that also processes governmental information, operates the deployed service, or independently reuses information shall be evaluated for each function rather than solely as a product supplier. Where stacked roles create incompatible duties, the more protective duty shall not be disregarded; the function SHALL be segregated, restructured, or governed by a more specific controlling law sufficient to resolve the conflict.

SECTION 26. LIFECYCLE ALGORITHMIC IMPACT ASSESSMENT

(a) Tier I systems and material Tier II systems SHALL undergo periodic AIA at intervals proportionate to consequence and change, and at least annually unless DTA regulation establishes a different risk-based interval.

(b) The AIA SHALL evaluate actual performance, errors, false positives and negatives where relevant, disparate outcomes, drift, material incidents, overrides, appeals, corrections, security, ACD, unauthorized capability, Vendor changes, and continued legal authority. Evaluation metrics SHALL be appropriate to the governmental function and shall not be treated as interchangeable across materially different populations or consequences.

(c) A material adverse finding SHALL produce a documented remediation decision, including modification, narrowed use, additional review, suspension, or retirement as appropriate.

(d) The DTA may order independent testing or remediation where agency testing is insufficient.

(e) Material systematic error affecting past governmental decisions SHALL trigger an assessment of notice, reopening, correction, or other retrospective remedy consistent with PDTA and applicable law.

SECTION 27. CIVIL-RIGHTS AND DISPARATE-OUTCOME TESTING

(a) Tier I systems SHALL be evaluated for unlawful discrimination and material disparate outcomes across legally protected groups where the data, sample size, governing law, and governmental function permit a methodologically valid evaluation.

(b) A statistical disparity is not by itself a violation of this Act unless applicable civil-rights law or another provision of law so provides. A material disparity identified through a methodologically valid evaluation SHALL trigger documented investigation for error, proxy discrimination, unjustified features, data-quality problems, or unlawful governmental criteria and remediation where a violation or material system defect is found.

(c) Testing methodology SHALL be appropriate to sample size, base rates, consequence, and applicable legal standards.

(d) Nothing in this section authorizes collection, retention, or operational use of protected-class information otherwise prohibited by law. Where lawful, agencies may use controlled evaluation datasets, privacy-preserving testing, statistically valid external benchmarks, or other methods segregated from operational decision-making.

SECTION 28. DRIFT, CHANGE MANAGEMENT, AND REAUTHORIZATION

(a) Agencies SHALL monitor material drift in data, model behavior, system use, population, tools, external services, and decisional consequences.

(b) A material change affecting purpose, authority, informational operations, features, population, model materiality, or consequence requires reassessment and, where applicable, renewed authorization or an updated AADA.

(c) Vendor model updates SHALL not be deployed automatically into material governmental use without controls sufficient to determine whether the update is material.

(d) Tier drift is governed by Section 7.

SECTION 29. AGENTIC SYSTEMS AND TOOL-USING AI

(a) An Agentic System is a technical agent, not an independent legal fiduciary or source of authority.

(b) Every tool, data source, query, disclosure, transaction, and external action available to an Agentic System SHALL be bounded to the originating Legitimate Informational Authority of the governmental function it serves. Tool availability, delegated credentials, or downstream system capability does not expand that boundary.

(c) Agentic Systems SHALL use least-privilege technical permissions and SHALL NOT receive generalized credentials or standing cross-purpose access merely for operational convenience.

(d) Material external actions SHALL be logged with sufficient provenance to reconstruct the authority, tool invocation, information used, and resulting effect.

(e) Where an agent can materially expand its own accessible tools, data, permissions, or objectives, such self-expansion SHALL be technically constrained or require a new authorization event.

(f) Government and responsible Vendors remain accountable for agentic conduct within capabilities they provide.

(g) Agentic Capability-Chain Inheritance

A delegated subagent, model, tool, credential, retrieval service, external API, or downstream automated action invoked by an Agentic System inherits the Originating Informational Purpose, Positive Legal Authority, Legitimate Informational Authority, Purpose-Divergence, informational-operation, information-domain, duration, permitted-consequence, Necessary Standing Informational Capability, and Exception Envelope boundaries applicable to the originating task. Delegated technical permission SHALL be least-privilege and non-transitive unless independently authorized and justified. An Agentic System SHALL NOT obtain materially broader capability by invoking another actor, system, Vendor, or service that possesses broader Standing Technical Informational Capability. Material credential propagation and downstream tool delegation SHALL be attributable and auditable.

SECTION 30. CITIZEN-FACING ASSISTIVE AI

(a) A citizen-facing AI system SHALL clearly disclose automated operation where a reasonable person could otherwise believe the system is a human government employee or the final authoritative decision-maker.

(b) A person SHALL have a reasonably accessible route to human assistance where necessary to exercise a legal right, contest material information, resolve system failure, or obtain a service that cannot lawfully be conditioned on exclusive AI interaction.

(c) An assistive system SHALL NOT represent nonbinding guidance as a final legal determination.

(d) Material information supplied by a citizen-facing system shall, where reasonably practicable, be grounded in authoritative governmental sources.

(e) Agencies SHALL monitor material recurring errors and promptly correct authoritative content or system behavior within their control.

SECTION 31. ACCURACY, OFFICIAL-SOURCE GROUNDING, AND RELIANCE

- (a)** Accuracy safeguards SHALL be proportionate to the consequence of foreseeable error.
- (b)** Where a Tier III system provides individualized legal, benefits, licensing, deadline, eligibility, or compliance guidance, the agency SHALL identify authoritative source material or provide an accessible means to verify material statements.
- (c)** A disclaimer does not cure deployment that government knows or should know is materially unreliable for the represented function.
- (d)** Nothing in this section creates an entitlement to rely on informal automated guidance contrary to controlling law unless applicable law otherwise provides; remedies for harmful government error remain governed by PDTA, this Act, and other applicable law.

SECTION 32. SYNTHETIC MEDIA AND AUTHENTICITY

- (a)** Government-generated synthetic audio, video, imagery, or impersonation-capable media used in public communications SHALL be disclosed or authenticated in a manner appropriate to prevent material deception, except where lawful covert use is independently authorized.
- (b)** Government SHALL not treat synthetic media as authenticated evidence merely because an Algorithmic System generated or classified it.
- (c)** VIDA governs identity-authentication architecture; this Act governs algorithmic generation, detection, or use of synthetic media.
- (d)** DTA regulations may establish provenance or authenticity requirements for high-consequence governmental synthetic media.

SECTION 33. PROCUREMENT AND VENDOR OBLIGATIONS

- (a)** Procurement SHALL require the least informationally powerful computational and informational functions reasonably sufficient for the legitimate standing governmental use, not generalized capability merely because broader capability is positively authorized, commercially bundled, technically convenient, or potentially useful in a future circumstance.
- (b)** Contracts for material systems SHALL require documentation and access rights sufficient for AADA, AIA, explanation, audit, provenance, testing, change management, security, regulator access, records preservation, transition, and termination. A Vendor may protect trade secrets and proprietary information from public disclosure as provided by law, but contractual secrecy SHALL NOT prevent government from satisfying its legal duties or the DTA from obtaining information it is legally authorized to receive.
- (c)** Vendors SHALL promptly disclose material known defects, incidents, model changes, or limitations reasonably likely to affect lawful governmental use.
- (d)** A Vendor SHALL NOT use governmental information for independent model training, product improvement, profiling, sale, or unrelated use except where independently authorized by law and contract.
- (e)** Government SHALL retain sufficient exit rights to discontinue a nonconforming system without loss of governmental records, audit evidence, or essential continuity.
- (f)** Contract terms SHALL not prevent the DTA from obtaining information necessary to exercise lawful oversight.
- (g)** Material procurement SHALL identify Positive Legal Authority, Standing Legitimate Informational Authority, Necessary Standing Informational Capability, Standing Technical

Informational Capability, the Authority-Capability Delta, narrower architectural alternatives, and any bundled capability that must be removed, disabled, segregated, or made available only after a new predicate or Materially Renewed Authorization.

SECTION 34. INDEPENDENT INFORMATION INTERMEDIARIES AND CAPABILITY LAUNDERING

(a) Government SHALL NOT use a Vendor, Independent Information Intermediary, model provider, commercial data source, or governmental partner to obtain informational or decisional capability it could not lawfully and conformingly exercise directly for the relevant function. Outsourcing does not enlarge Legitimate Informational Authority or Necessary Standing Informational Capability.

(b) Informational transformation by a third party does not cleanse an unauthorized governmental acquisition or inference.

(c) A model trained on broadly available commercial information may be used only to the extent the governmental deployment and resulting knowledge satisfy PDTA and this Act.

(d) Government SHALL assess whether external AI services retain prompts, outputs, embeddings, tool calls, or other metadata in a manner that creates unauthorized disclosure, profiling, or reacquisition risk.

SECTION 35. DTA OVERSIGHT AND TECHNICAL COMPETENCE

(a) The Data Trusteeship Authority established by PDTA is the principal independent oversight and enforcement authority for this Act.

(b) The DTA SHALL maintain or obtain expertise in machine learning, statistics, software engineering, cybersecurity, privacy engineering, civil rights, administrative law, government operations, human factors, and other disciplines necessary to evaluate covered systems.

(c) The DTA may convene independent technical experts or an advisory panel, but advisory bodies do not displace DTA accountability or exercise independent enforcement authority unless separately authorized by law.

(d) The DTA may conduct or require audits, red-team testing, negative-capability testing, model evaluations, documentation review, and other technically appropriate assessments.

(d-1) Remedial and Operational Boundary

The DTA may establish or order the legal and conformance outcome necessary to cure a violation, including suspension, limitation, testing, removal of unauthorized Features or data sources, explanation or human-review safeguards, and retirement of prohibited capability. Except where necessary to enforce a final lawful order or expressly authorized by law, the DTA shall not select ordinary agency AI products, operate production models, tune models for agency missions, or substitute itself for the operational authority of the State CIO or Responsible Government Agency.

(e) Oversight systems SHALL themselves comply with PDTA and SHALL not create unnecessary population-scale analytical repositories.

SECTION 36. CONFORMANCE, RULEMAKING, AND TECHNICAL STANDARDS

(a) The DTA may adopt binding conformance regulations implementing this Act consistent with PDTA. Regulations SHALL implement, and shall not enlarge, the substantive governmental authority or prohibited capability established by enacted law.

(a-1) Trilogy Conformance Code

Binding algorithmic and AI conformance regulations adopted under this Act SHALL be maintained within the PDTA Trilogy Conformance Code and public version registry. AI-specific profiles may specify AADA, AIA, provenance, testing, model-materiality, learned-artifact, agentic-system, or explanation evidence but SHALL remain traceable to enacted law and the controlling Code version.

(a-2) FCGIAS Reference Integrity

Any FCGIAS AI, analytics, model, agentic-system, or conformance control used as a binding requirement SHALL be incorporated and traceable in the manner required by PDTA Section 25. FCGIAS, a reference implementation, control catalog, model card, evaluation methodology, or Normative Traceability Matrix does not independently create Governmental Informational Authority, a Tier classification, a private cause of action, an exception, or a substantive Vendor duty.

(b) The State CIO or equivalent executive technology official may issue operational technical standards consistent with enacted law and DTA regulations. Such standards may govern implementation, interoperability, security, testing, documentation, and procurement but SHALL NOT independently create governmental informational authority, diminish statutory rights, or establish exceptions to substantive prohibitions.

(c) Regulations shall specify functional outcomes and conformance requirements rather than mandate particular model families, Vendors, programming techniques, or technical standards unless specification is reasonably necessary to implement enacted law.

(d) Conformance SHALL be based on actual capability and use, including hidden or composite integration through APIs, tools, agents, retrieval systems, metadata, Vendors, and external services, and SHALL determine whether Standing Technical Informational Capability materially exceeds Necessary Standing Informational Capability or Standing Legitimate Informational Authority.

(e) Structural nonconformance is non-compensable by documentation, encryption, or audit alone where prohibited or unnecessary standing capability remains available through ordinary access.

(f) Regulatory Non-Bootstrap and Express Legislative Departure

The DTA and State CIO may implement enacted legitimacy and capability criteria but may not create Governmental Informational Authority, relax Structural Least-Power requirements, or treat FCGIAS or another technical standard as an independent source of governmental power. A later statute may expressly supersede a requirement of this Act, but broad purpose language or generalized authorization SHALL NOT by implication repeal, waive, or satisfy a more specific informational-legitimacy requirement.

SECTION 37. TRANSPARENCY REGISTRY AND PROTECTED INFORMATION

(a-1) Common Rule

Transparency and protected-information treatment under this section shall be construed consistently with the common PDTA transparency and protected-information rule. Public accountability SHALL be sufficient to identify material covered systems, governmental function, tier, Responsible Government Agency, general classes of data and outputs, and available rights and review mechanisms, while preserving independently protected security, privacy, privilege, source, investigative, procurement, and trade-secret interests. Withholding shall be no broader or longer than independently applicable law permits.

(a) The DTA SHALL maintain or designate a public registry of material governmental Algorithmic Systems sufficient to identify the deploying agency, system function, tier, general purpose, affected population or domain, Vendor where applicable, and current deployment status.

(b) Tier I AADA summaries and material Tier II AADA summaries SHALL be public subject to lawful redaction. The DTA may require publication of a full AADA where public disclosure is required by law or where the agency elects to publish it; nothing in this Act overrides independently applicable public-records exemptions or disclosure obligations.

(c) Redaction or withholding SHALL rest on independently applicable law and may protect security-sensitive information, privileged material, confidential sources, protected personal information, active investigative information, procurement-sensitive information, and trade secrets. Agencies SHALL disclose reasonably segregable nonexempt information sufficient for public accountability.

(d) The existence of a material system, its governmental function, tier, and responsible agency SHALL not be withheld solely because the Vendor asserts confidentiality, except where another law independently authorizes withholding.

(e) The DTA SHALL have access to unredacted information necessary for lawful oversight, subject to applicable security restrictions.

SECTION 38. AUDITABILITY, RECORDS, AND PRESERVATION

(a) Agencies SHALL maintain records sufficient to demonstrate compliance and reconstruct material Tier I decisions and material Tier II analytical escalations.

(b) Audit requirements SHALL be proportionate and need not require indefinite retention of every intermediate token, model state, or computational artifact where such retention is unnecessary to accountability.

(c) Preservation authority is distinct from operational processing authority. A legal hold or records obligation does not authorize continued unrelated model use.

(d) Audit records may be correlated for independently authorized oversight and abuse detection consistent with PDTA.

SECTION 39. ENFORCEMENT AND REMEDIES

(a) Private and Public Enforcement. A person materially affected by a violation of Sections 5 through 32 may obtain relief through PDTA Sections 20 through 24 where the violated provision creates or protects an individual substantive right, prohibits an informational or automated operation materially affecting the person, or expressly imposes a privately enforceable Vendor duty. Failure to complete an AADA, AIA, classification, audit, registry, procurement, reporting, or other institutional requirement does not, standing alone, create a private damages claim unless this Act expressly provides otherwise, but may be enforced by the DTA or Attorney General and may constitute evidence of an independently enforceable violation. Section 33 does not independently create a private cause of action solely for breach of a procurement, contracting, documentation, audit-access, or other institutional Vendor obligation; conduct governed by Section 33 remains privately enforceable to the extent the same conduct violates an independently privately enforceable duty under PDTA, Sections 5 through 32 of this Act, VIDA where applicable, or other law.

(b) GAAFA-specific structural relief may include suspension of a model or function, removal of unauthorized or unnecessary features or data sources, disabling unauthorized inference or correlation, narrowing tool permissions, transactionalizing broader capability, requiring a predicate or Materially Renewed Authorization before activation, segregating capability,

disabling bundled capability, requiring human review, requiring de novo reconsideration, correcting Derived Information, reopening materially affected determinations, or retiring a nonconforming system.

(c) Where competent evidence establishes a reasonable basis to conclude that systematic error or unlawful model use materially affected a class of prior governmental decisions, the DTA or a court, within the remedial authority granted by PDTA and other applicable law, may require a proportionate retrospective identification and remediation process. Any reopening, repayment, recoupment, finality, limitations, notice, or reliance consequence remains subject to independently applicable law.

(d) Nothing in this Act creates a private claim against software itself.

(e) Rights and remedies are cumulative to the extent provided by PDTA and other applicable law.

SECTION 40. LEGACY SYSTEMS AND TRANSITION

(a) PDTA Transition Controls

PDTA Section 28 supplies the generally applicable transition, Legacy Structural Remediation Safe Harbor, remediation-duration, and existing-contract framework for systems governed by this Act.

(b) AI-Specific Inventory and Classification

Within the period established by PDTA or binding DTA regulation, existing material Algorithmic Systems SHALL be inventoried and classified under Section 7, including material models, agents, data and Feature sources, learned or derived computational artifacts, Vendor dependencies, and known structural nonconformance.

(c) New or Materially Changed Systems

Beginning on the general effective date, no Government Agency may newly deploy or materially expand an Algorithmic System in violation of the substantive authority, purpose, anti-laundering, Tier I safeguard, or other immediately applicable requirement of this Act. New or materially changed systems SHALL complete required predeployment assessment before the changed use begins.

SECTION 41. PERIODIC REVIEW

(a) Consolidated Review Cycle

Review of this Act shall occur within the coordinated PDTA Section 26 trilogy review. This section does not establish a separate general review cycle.

(b) AI-Specific Subjects

The coordinated review SHALL address tier classification; agentic systems and capability chains; model and data developments; statewide analytics; explanation and contestability; civil-rights testing; commercial AI services; synthetic media; learned computational artifacts; Relational Information; cybersecurity and abuse-detection analytics; model training and cross-purpose reuse; conformance experience; circumvention mechanisms; FCGIAS reference integrity; and harmonization with PDTA and VIDA.

(c) Technical and Public Participation

The AI portion of the coordinated review SHALL include meaningful participation by affected individuals, civil-rights and privacy organizations, state and local agencies, statisticians, machine-learning and software engineers, cybersecurity professionals, administrative-law and

civil-rights experts, human-factors specialists, Vendors, procurement officials, and other materially affected stakeholders.

(d) No Automatic Sunset

The review requirement does not sunset this Act.

SECTION 42. SEVERABILITY

(a) If any provision of this Act or its application is held invalid, the remaining provisions and applications remain effective to the maximum extent possible.

(b) Invalidity of a particular technical or procedural requirement does not invalidate the underlying requirements of lawful authority, boundary inheritance, meaningful accountability, contestability, or prohibition on generalized informational capability.

(c) Provisions governing Tier I decisions, Tier II analytics, Tier III assistance, Vendors, and oversight are severable to the extent they can operate independently.

SECTION 43. EFFECTIVE DATE

(a) This Act takes effect [180] days after enactment.

(b) The DTA and State CIO may undertake rulemaking, inventories, standards development, procurement preparation, staffing, and implementation immediately upon enactment.

(c) Transactional duties capable of immediate compliance become enforceable on the general effective date.

(d) Structural transition is governed by Section 40.

(e) No legacy system, model, contract, commercial service, or technical capability acquires Governmental Informational Authority merely because it existed before enactment.

GOVERNING CONSTRUCTION

AI may increase government's capacity to execute lawful authority; it does not enlarge that authority.

Technical ability to infer does not create authority to infer.

Scale concerns how many records are processed. Generality concerns how unconstrained the governmental informational question is.

A hypothesis is not an adjudicative fact.

Human presence is not meaningful human judgment.

A commercial model's lawful possession or generation of information does not establish government's authority to know or use it.

Composite automation is assessed by the governmental capability and consequence of the whole workflow, not by the label attached to each component.

Government should be able to use powerful computational tools for legitimate purposes without acquiring standing generalized power to know or decide materially more than law authorizes.

Positive Legal Authority is necessary but is not self-validating as to the legitimacy or necessity of every computational capability.

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

Predictive utility does not create Legitimate Informational Authority.

Tool availability does not enlarge an Agentic System's inherited legitimacy boundary.

Authority is an outer ceiling on governmental informational power, not a specification for the maximum computational capability government should procure or maintain as ordinary standing power.

END OF GAAFA VERSION 2.2 - CLEAN RESTATED LEGISLATIVE CANDIDATE

APPENDIX A - SECTION-LEVEL NORMATIVE TRACEABILITY

This appendix is interpretive and traceability-oriented. It does not independently create governmental authority, rights, duties, exceptions, or liability. It identifies the principal upstream source for each GAAFA section, including the FCGIAS Version 2.2 Candidate Standard and the adopted IR-01 Structural Least-Power clarification.

Version 2.2 Supplemental Traceability

T-61 through T-63 → Sections 2, 5, 9, 10, 11, 19, 29, 33, and 36: PLA/LIA separation, originating purpose, and inherited AI authority boundaries.

T-64 through T-66 → Sections 5, 9, 10, 11, 19, and 20: Purpose Divergence, Informational Justification Level, and Anti-Abstraction.

T-67 through T-69 → Sections 12, 20, 29, 34, and 36: no positive-authority bootstrap, relational legitimacy, Vendor/intermediary non-expansion, and conformance-legality separation.

T-70 / CF-79 / SD-13 → Sections 2, 5, 9, 12, 21, 29, 33, 36, and 39: Necessary Standing Informational Capability, Structural Least Power, bundled-capability control, and least-power remediation.

GAAFA	Primary upstream rule	FCGIAS / architecture control	Principal legal function
§ 1	PDTA statutory framework	-	Title
§ 2	PDTA Ordered Informational Authority / LIA / ACCP	ACCP; Structural Least Power; AI boundary inheritance	Findings and governing principle
§ 3	PDTA/VIDA definitions	Derived information; model materiality	Computational ontology
§ 4	PDTA authority; VIDA identity boundary	Normative hierarchy	Trilogy allocation
§ 5	PDTA capability ≠ authority; LIA	AI Boundary Inheritance; T-70 / CF-79	Institutional accountability
§ 6	PDTA operation-specific authority	Authorization operations	Separate informational operations
§ 7	PDTA material expansion	Model Materiality; Analytics-Adjudication Separation	Tier classification
§ 8	PDTA proportional controls	Tier controls	Baseline safeguards
§ 9	PDTA PLA / LIA / OIP / Purpose Divergence / ACΔ	AADA; IJ Level; Authorized Answer; negative testing	Predeployment assessment
§ 10	PDTA Purpose / Question Particularity;	Question Particularity;	Bound analytical

	Anti-Abstraction	LIA boundary	question
§ 11	PDTA legitimacy / necessity / derived information	Feature Authority; learned-artifact divergence; provenance	Inputs/model authority
§ 12	PDTA Vendor Non-Expansion / nondelegation	Assessment Boundary; conformance attribution	Vendor assessment
§ 13	PDTA III rules	Commercial availability; transformation	Commercial outputs
§ 14	PDTA accountability/due process	Meaningful Human Judgment	Human decisional accountability
§ 15	PDTA transparency/contest ability	Provenance; epistemic status	Explanation
§ 16	PDTA transparency	Decision notice	Notice
§ 17	PDTA correction/contestability	Independent review	Contest
§ 18	PDTA correction	Derived Information Correction	Correction propagation
§ 19	PDTA inference legitimacy	Material Derived Inference; predictive utility insufficient	Inference
§ 20	PDTA Bounded Government Discovery / IJ-4	Objective predicate; generalized-capability presumption	Discovery
§ 21	PDTA purpose sequestration	Purpose-Bounded Analytics Enclave	Cross-domain analytics
§ 22	PDTA derived info	Epistemic Status	Hypothesis outputs
§ 23	PDTA permitted consequence	Analytics-Adjudication Separation	No signal-to-sanction shortcut
§ 24	PDTA retention/preservation	Signal Retention; transient integration	Computational retention
§ 25	PDTA anti-circumvention	Model Materiality; Composite Machine Action	End-to-end assessment
§ 26	PDTA continuous	AIA; continuous	Lifecycle review

	conformance	conformance	
§ 27	Applicable civil-rights law + PDTA care	Outcome testing	Bias/disparity evaluation
§ 28	PDTA material expansion	Change management	Drift/reauthorization
§ 29	PDTA AI-agent rule / LIA	Capability-chain inheritance; least privilege; T-70	Agentic systems
§ 30	VIDA digital autonomy/access	Citizen-facing AI	Human escalation
§ 31	PDTA care/transparency	Official-source grounding	Accuracy/reliance
§ 32	VIDA authenticity + GAAFA computation	Synthetic authenticity	Synthetic media
§ 33	PDTA procurement / Vendor rules / Structural Least Power	Procure necessary capability; disable bundled excess	Procurement
§ 34	PDTA III/capability laundering	Reacquisition loop	External AI/data
§ 35	PDTA DTA authority	Independent conformance	Oversight
§ 36	PDTA regulatory hierarchy / non-bootstrap	FCGIAS 2.2; CF-79; structural noncompensability	Rulemaking/ standards
§ 37	PDTA transparency/public records	Transparency with bounded disclosure	Registry
§ 38	PDTA audit/preservation	Audit separation; preservation distinction	Records
§ 39	PDTA remedies	Least-Power Remedy; IR-01 sequence	Enforcement
§ 40	PDTA legacy safe harbor	Continuous conformance	Transition
§ 41	PDTA review	Continuous conformance	Periodic review
§ 42	General statutory construction	Technology independence	Severability
§ 43	PDTA transition	No grandfathered authority	Effective date

APPENDIX B - LEGISLATIVE DRAFTING NOTES AND STATE-SPECIFIC FILL-INS

Replace [Legislative Body] and state-office placeholders with the enacting jurisdiction's terminology.

Confirm DTA placement, appointment, subpoena, rulemaking, and judicial-review provisions against the enacting State's administrative-procedure and separation-of-powers law.

Conform private-right-of-action, sovereign-immunity, damages, attorney-fee, limitations, and court-jurisdiction provisions to the finalized PDTA enactment.

Set the bracketed implementation periods after inventorying current state AI systems and procurement cycles.

Cross-reference the enacting State's public-records, records-retention, procurement, civil-rights, administrative-hearing, criminal-procedure, and emergency-management statutes.

Do not incorporate a named NIST AI RMF version as binding law. DTA/CIO standards may use current NIST resources as informative technical references without permitting those resources to enlarge or diminish enacted rights or authority.