LEGISLATIVE ADVOCACY WHITE PAPER

Building the Trustworthy Digital State:

The Case for Enacting VIDA and PDTA Together

Verifiable Identity and Digital Autonomy Act (VIDA) **Personal Data Trusteeship Act (PDTA)** *A Comprehensive Framework for Security, Utility, and Constitutional Compliance in Digital Government Services*

Prepared by Michael G. Leahy

March 2026

Executive Summary

State governments across America face a convergent crisis: centralized digital infrastructure built for administrative convenience has become a liability: constitutionally suspect, financially costly, and increasingly attractive to adversaries. High-profile breaches, expanding surveillance architectures, and an authentication crisis driven by artificial intelligence are not independent problems. They share a common root: the accumulated data concentrated in government systems has made agencies both the target and the source of harm.

The Verifiable Identity and Digital Autonomy Act (VIDA) and the Personal Data Trusteeship Act (PDTA) address this crisis at its root. VIDA mandates decentralized, citizen-controlled digital identity infrastructure governed by cryptographic standards and fiduciary duties. PDTA establishes individuals as trustees over their own personal data, imposing binding fiduciary obligations on every government actor that handles that data. Enacted together, they transform the digital relationship between government and citizen: from surveillance-capable data warehouse to constitutional trustee; from single-point-of-failure architecture to distributed resilience; from administrative opacity to auditable accountability.

The Problem Today	**The VIDA + PDTA Solution**
Centralized databases: single points of catastrophic breach	Distributed, individual-held credentials: no single attack

surface |
Data shared across agencies without purpose limitation	Purpose-sequestered databases; lateral access prohibited
Citizens uninformed about who accesses their records	Individual-controlled, immutable audit trails for all access
AI-generated deepfakes can defeat identity verification	Cryptographic signatures render the presentation medium irrelevant
Only 33% of Americans trust federal government with data	Fiduciary duties create legally enforceable trust obligations
Constitutional exposure under the Fourth Amendment	Architecture aligned with the Amendments performance. VIDA and PDTA translate this constitutional requirement into enacted law.

The Security Deficit

Centralized databases are not merely constitutional liabilities. They are catastrophic security risks. The aggregate of personally identifiable information held by state and federal agencies (tax records, benefits data, licensing files, vital statistics, and criminal histories) represents a prize of extraordinary value to adversaries. When centralized repositories are breached, the damage is comprehensive and irreversible.

Recent incidents illustrate the scale of this vulnerability. In 2025 alone, a zero-day exploit in Microsoft SharePoint compromised sensitive data across federal and state agencies. The National Public Data breach exposed Social Security numbers and personal records of nearly 2.9 billion individuals. Major breaches at Ascension Health and AT&T exposed millions of records, disrupting services and eroding public confidence. These are not isolated failures. They are the predictable consequence of centralization: concentrate the data, concentrate the risk.

| **The Security Logic of Decentralization** When individuals hold their own credentials rather than government maintaining centralized repositories, no single breach yields comprehensive fraud capability. Each credential must be individually compromised, which is a categorically harder attack than breaching a single database. Mutual cryptographic authentication, in which both citizen and agency verify each others private cryptographic key can be verified by anyone against the governments fundamental interests and is legally accountable for that stewardship, provides exactly this structural foundation. VIDA and PDTA impose fiduciary duties not as aspirational policy

but as enforceable law with private rights of action, statutory damages, and consequences paid from agency operating budgets.

II. VIDA: Decentralized Identity as Constitutional Architecture

Core Framework

The Verifiable Identity and Digital Autonomy Act establishes the technical and legal architecture for citizen-controlled digital identity in government services. Its core mandate is simple but transformative: government may endorse identity, but may not create or centrally maintain it. This distinction, with constitutional significance, inverts the traditional issuer-subject relationship. When government issues identity documents in the traditional framing, the language implies identity flows from sovereign grant. Endorsement reverses this relationship: individuals possess identity as a constitutional and existential fact; government cryptographically certifies claims individuals make about themselves.

Decentralized Identifiers and Verifiable Credentials

VIDA mandates the use of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) based on open standards published by the World Wide Web Consortium. A DID is a cryptographically derived identifier under the sole control of the individual, requiring no centralized registry. A VC is a cryptographically signed assertion by an issuer (such as a state agency attesting to age, residency, or licensure) held by the individual in a personal digital wallet and presented selectively as needed.

The practical implication is profound. Instead of a verifier querying a government database to confirm that an individual holds a valid drivers reasonableness standard: where verification suffices, collection is unreasonable. It also eliminates the data retention burden and breach risk associated with collection, creating both fiscal and security benefits that compound over time.

Zero Trust Architecture

VIDA requires all identity verification and access control systems to operate under Zero Trust Architecture, the principle that no user, device, or system is trusted by default, regardless of network position. Every identity assertion is independently

verified through cryptographic means without persistent state or assumed prior relationships. Shared secrets, passwords, and knowledge-based authentication are prohibited. Multi-factor authentication relying on centralized device-bound factors is replaced with cryptographic, decentralized, holder-controlled authentication.

This mandate closes the security vulnerabilities that legacy systems perpetuate. Password databases are eliminated as attack surfaces. Phishing attacks that harvest shared secrets become ineffective. Insider threats requiring centralized database access are constrained. The architecture assumes breach at every layer and verifies cryptographic authorization independently, so the compromise of any single component cannot cascade into comprehensive system failure.

Purpose-Sequestered Databases

VIDA bans centralized multipurpose data lakes and requires all personal data to be stored in discrete, sequestered, purpose-specific datasets enforcing Zero Trust principles. An individuals licensing is isolated from benefits data, tax data, and law enforcement data. Lateral access across datasets is prohibited. Each use is independently auditable with retention limits tied to the specific legal purpose that justified collection.

**VIDA Duty of Care: Implement appropriate security, transparency, and governance practices to protect data integrity and confidentiality. Duty of Portability: Enable individuals to access, download, and transfer their data and credentials without undue hindrance.

**VIDAs obligations are backed by an enforcement architecture designed to ensure accountability without requiring government self-policing. A Data Fiduciary Oversight Office investigates complaints, enforces fiduciary obligations, publishes transparency reports, and imposes penalties including suspension of procurement eligibility and public disclosure of non-compliance. The Attorney General holds independent enforcement authority.

Critically, all penalties are paid from the operating budgets of agencies found in violation, not from the general fund. This creates institutional incentives for compliance that abstract statutory obligations cannot match. Agency leadership has direct

financial interest in maintaining fiduciary standards. Officers and employees found to have committed willful violations cannot be indemnified with public funds. Private rights of action enable affected individuals to bring civil claims for injunctive relief, statutory or actual damages, and attorneys particularity requirement in statutory form.

This structure prevents the "routine use" doctrine that has effectively gutted Privacy Act protections, under which agencies currently define "compatible purpose" so broadly that almost any use within a vague agency mission qualifies. Under fiduciary analysis, purpose compatibility is strictly construed: materially different uses require new authorization, not administrative rationalization. A benefits agency that shares a recipients Enhanced Fiduciary Obligations**

PDTA recognizes that governments specific data commitments as an enforceable contract before any data is collected. The portal queries only what law requires, using zero-knowledge proofs where facts can be verified without transmission of underlying data. All steps are logged in an audit trail the citizen controls. The issued benefit credential is stored in the citizens information requires fresh authorization traceable to a specific legal purpose. |
| --- |

IV. How VIDA and PDTA Work Together

VIDA and PDTA are designed as complementary halves of a unified constitutional architecture. VIDA provides the technical infrastructure: the cryptographic identity systems, the decentralized credential framework, the Zero Trust protocols, and the purpose-sequestered databases. PDTA provides the legal superstructure: the fiduciary duties, the trusteeship rights, the enforcement mechanisms, and the individual remedies. Together, they create a system in which technical capability and legal obligation reinforce each other at every point.

Technical-Legal Integration

Consider a concrete example. A state resident applies for unemployment benefits. Under VIDA, the portal does not collect a birth date, Social Security number, and employment history and store them in a centralized benefits database. It queries the residents wallet.

Under PDTA, the portal presents binding commitments before any data is collected: data minimization, purpose sequestration, audit trail access, breach remedies with specified statutory damages. These commitments are enforceable contracts. The benefit credential is issued to the residents loyalty duty is violated and the resident has a private right of action.

Mutually Reinforcing Protections

VIDA Provides	**PDTA Provides**
Decentralized identity infrastructure mandating DIDs and VCs	Legal framework designating citizens as primary data trustees
Cryptographic zero-knowledge proofs for query-without-collection	Prohibition on repurposing data beyond original justified purpose
Zero Trust Architecture eliminating shared secrets	Bilateral trust structure limiting government to secondary fiduciary role
Purpose-sequestered databases prohibiting lateral access	Presumption favoring individuals in disputes with government agencies
Individual-held credentials eliminating central attack surfaces	Immutable audit trails under citizen control for all data interactions
Data Fiduciary Oversight Office with enforcement powers	Data Trusteeship Authority with audit, penalty, and remediation authority
Private right of action for fiduciary duty violations	Sovereign immunity waiver enabling monetary awards against government
Anti-deepfake cryptographic authentication standards	Enhanced government duty to counter AI-enabled surveillance threats

Addressing Emerging Threats Together

The bills also establish a framework for addressing threats that neither could adequately address alone. Agentic AI systems, which are autonomous agents acting on behalf of users or government in data transactions, present novel fiduciary challenges. VIDA actions are verifiable and attributable. PDTAs delegation framework supports privacy-preserving identity presentation by minors, dependents, and legal proxies. PDTAs digital services, and disability accommodation that current law addresses poorly or not at all.

V. Return on Investment: The Fiscal Case for VIDA and PDTA

VIDA and PDTA require upfront investment in technical infrastructure, staff training, and system migration. This investment is not merely justified by constitutional obligation and security improvement. It generates measurable fiscal return that exceeds implementation costs across multiple categories.

Direct Cost Avoidance: Breach Remediation

The average cost of a government data breach in 2024 exceeded $9.9 million per incident, including forensic investigation, notification, credit monitoring, regulatory response, litigation, and reputational damage. State agencies managing benefits, licensing, vital records, and tax administration hold data attractive to adversaries and face breach risk that grows as centralized repositories expand.

Decentralized individual-held credential architecture eliminates the centralized repositories that create catastrophic breach exposure. When individuals hold their own credentials, a breach of a government system yields no usable personal data, because that data is simply not there. Early adopters of decentralized identity systems have documented 60–70% reductions in identity fraud in benefits programs. The fiscal value of breach avoidance, applied across a states private key is not merely difficult; it is effectively impossible with current and foreseeable technology. States implementing VIDA-compliant identity verification in benefits administration can realistically project fraud reduction of 40–70%, generating fiscal savings that dwarf implementation costs.

Illustrative ROI Categories for State Implementation
ROI Category	**Basis / Documented Evidence**
Breach remediation cost avoidance	**$9.9M+ per incident avoided**
Benefits fraud reduction (40s cryptographic verification architecture replaces manual review with near-instantaneous cryptographic confirmation: the credential is valid, the eligibility criterion is met, or it is not. No manual review is required. No database query is necessary. No wait time for cross-agency verification.

Early implementations of verifiable credential systems in health assistance programs have documented processing time reductions of 60–80% for eligibility determinations, with corresponding reductions in administrative staff costs. Scaling these efficiencies across a states implementation timeline provides 24 months for new or re-platformed services and 48 months for retrofitting existing services, with waiver provisions for documented hardship. A grant program, funded through appropriations, assists agencies in adopting compliant systems. Agencies demonstrating full compliance through independent audits receive priority in digital initiative funding. The phased timeline distributes costs and allows agencies to sequence migration according to fiscal capacity while prioritizing high-risk areas first.

The open standards mandate, which requires all identity infrastructure to comply with W3C VC and DID specifications and be available on fair, reasonable, and non-discriminatory terms, prevents the vendor lock-in that has inflated costs in prior digital government initiatives. Competitive procurement under open standards consistently yields lower costs than proprietary systems. The mandate that penalties are paid from agency operating budgets rather than the general fund creates institutional pressure for compliance that reduces the likelihood of costly enforcement actions.

VI. Benefits for Government Agencies

Security

For agency administrators and chief information security officers, VIDA and PDTA offer the most consequential security improvement available: elimination of the centralized repositories that create catastrophic breach exposure. The bills do not require agencies to build better security around existing databases. They require replacing the architectural pattern that makes breaches catastrophic.

Zero Trust Architecture, mandated by VIDA, addresses insider threat, credential theft, and lateral movement, the attack vectors responsible for the most damaging recent breaches. Purpose-sequestered databases limit the blast radius of any single breach to data held for a single purpose. Individual-held credentials mean that compromising a government system yields no personal data to exploit.

Cryptographic mutual authentication defeats the impersonation attacks of spear phishing, social engineering, and deepfake-mediated fraud that currently defeat multi-factor authentication systems. For agencies responsible for protecting sensitive data under FISMA, NIST frameworks, and state security standards, VIDA compliance is not an additional burden. It is the path to compliance with best practices that security standards already require but that legacy architectures make structurally impossible.

Utility and Operational Efficiency

VIDAs wallet supports all four interactions, with the citizen controlling what is disclosed to each.

PDTA credentials, adult children managing elderly parentss license renewal supports a benefit application, a professional license renewal, and a voter eligibility verification. Selective disclosure means the resident presents only what each specific transaction legally requires.

For populations who currently face barriers to digital services, including individuals with disabilities, those with limited English proficiency, and those with limited digital access, VIDAs architecture generates provide the evidentiary foundation for PDTAs fiduciary duties provide the legal obligation that makes VIDAs fiduciary architecture and the founding-era prohibition on digital general warrants. They are technically sound, mandating mature, deployed cryptographic standards that already underpin secure digital identity systems in multiple jurisdictions. They are fiscally responsible, generating documented return on investment through breach avoidance, fraud reduction, and administrative efficiency that exceeds implementation costs.

The urgency is real. The surveillance infrastructure against which these bills provide protection is expanding rapidly, accelerated by artificial intelligence tools that make aggregated databases far more analytically powerful than their architects designed them to be. The deepfake authentication crisis is not a future concern; it is a present threat that legislation must address now, before centralized architectures become further embedded and transition costs rise further.

| **The Legislative Imperative** *Enact VIDA and PDTA together.

Do not delay for incremental alternatives that address symptoms while leaving the architectural violation intact. The constitutional verdict on digital general warrants is not new. It has been waiting two and a half centuries for its application. The technology for compliance exists. The fiscal case is documented. The public demands it. The moment for action is now.*
|
| --- |

The authors invite legislative staff, agency counsel, and advocacy partners to contact us for technical assistance, model legislation analysis, implementation planning support, or expert testimony. The framework developed here represents not merely a policy proposal but a constitutionally grounded architecture for the digital relationship between state government and its citizens, one that serves both governance and liberty, both security and autonomy, both present efficiency and long-term constitutional fidelity.

About the Author

Michael G. Leahy is the author of Digital General Warrants: Why Government Databases Violate the Fourth Amendment and Government as Information Trustee: A Fiduciary Framework for Surveillance-Age Privacy. He serves as a policy advisor on digital identity, constitutional privacy architecture, and government data governance.