Technology as a Strategic Asset

A Statewide Technology Agenda for New Mexico's Next Administration

Peter Mantos
Mantos IT Consulting, Inc.
November 2026

Authorship, Independence and AI Disclosure

Prepared by Peter Mantos, Mantos IT Consulting, Inc. This document presents the independent analysis and recommendations of the author. It does not represent the views or policies of the State of New Mexico, any current or future administration, gubernatorial candidate, state agency, elected official, or other individual or organization unless expressly stated.

Generative artificial intelligence tools were used to assist with research, source discovery, analysis, editing and document preparation. The author directed the work, reviewed the supporting sources and resulting analysis, and accepts responsibility for the conclusions presented. Factual claims are supported by cited sources wherever practicable.

Executive Proposition

Source notation: Bracketed references such as [S6, S7] identify numbered sources in the companion document "Evidence Base & Source Map" which groups the sources by policy proposition and explains what each source supports, limits, or contradicts.

Technology is now part of the machinery through which nearly every major state policy is delivered. The question for New Mexico's next administration is not whether all information technology should be centralized. It is which technology capabilities should be governed and delivered at enterprise scale, and which should remain close to the agencies whose missions they implement.

> **Centralize what creates enterprise value. Preserve autonomy where mission specialization creates value.**

New Mexico already operates important statewide technology services, and recent state actions have strengthened enterprise cybersecurity, project oversight, and enterprise service planning. The next administration should build on that foundation and move the State materially along the continuum from fragmented agency-by-agency technology toward a deliberate hybrid enterprise model. **[S6, S7, S8, S9, S10]**

A five-year horizon is realistic for substantial movement, not complete centralization. The objective should be an enterprise-first model for common capabilities, coupled with strong agency ownership of mission systems and business rules.

This direction is supported by a broad body of public-sector and industry research. The National Association of State Chief Information Officers (NASCIO), the U.S. Government Accountability Office (GAO), Gartner, Forrester, and Accenture all describe movement toward shared services, enterprise standards, common platforms, or consolidation of common capabilities. Their guidance also consistently preserves exceptions where mission, legal, technical, or operational requirements justify local control. The resulting direction is not "centralize everything"; it is to consolidate and standardize where enterprise scale creates value and retain federation where mission specialization requires it. **[S1, S2, S3, S13, S14, S15]**

1. State IT Operates on a Spectrum

Public-sector technology organizations operate on a continuum. At one end, agencies independently select, build, operate, and secure most of their technology. At the other, common technology functions are governed and delivered centrally. The National Association of State Chief Information Officers (NASCIO) reported in 2024 that 90% of responding state CIO organizations were consolidating infrastructure, 69% were consolidating services, 63% were centralizing IT project management and oversight, and only 8% reported greater federation or decentralization of IT roles and personnel. NASCIO nevertheless cautions that not every state or capability will be fully consolidated. **[S1]**

For the detailed characteristics of each stage of the continuum—from Highly Decentralized through Federated, Coordinated Federated, Hybrid Enterprise, Enterprise-Led, and Highly

Consolidated—see companion Statewide Governance Model Spectrum Graphic. The graphic should be read as a capability-placement model, not as a requirement that every function move to the same point on the spectrum.

Federated	Coordinated Federated	Hybrid Enterprise	Enterprise-Led	Highly Consolidated
Agencies operate most technology independently.	Enterprise standards and selected shared services.	Common capabilities shared; mission technology remains agency-owned.	Most common IT governed and delivered enterprise-wide.	Most technology organization and delivery centralized.

New Mexico today: substantially federated for mission systems, with important enterprise services already in place

Five-year direction: move materially toward Hybrid Enterprise / Enterprise-Led for common capabilities

The policy goal should therefore not be "centralization" as an ideology. It should be the disciplined placement of each capability at the point on the spectrum where statewide scale, security, interoperability, consistency, or purchasing power create the greatest public value.

New Mexico evidence has sharpened the urgency. In an October 20, 2026 evaluation brief, the Legislative Finance Committee reported that the four largest ongoing state IT projects collectively exceeded their initial estimates by $456 million and identified major delays and shortcomings in delivered functionality. The finding concerns the four projects evaluated—not every state IT project—and supports stronger portfolio visibility, lifecycle oversight, and incremental delivery rather than any assumption that organizational consolidation alone will fix delivery performance. [S31]

2. IT Is Both Commodity and Strategic

Some technology is mature, standardized, and broadly available in the market. Internet access, email, office-productivity tools, printing, standard endpoint services, and routine infrastructure can often be sourced competitively with little effect on an agency's mission differentiation. Treating these capabilities as commodities is rational.

> **The mistake is not treating commodity IT as a commodity. The mistake is treating all IT as though it were a commodity.**

Most agencies also depend on one or more core systems that embody statutory requirements, business rules, workflows, and institutional knowledge. A tax-processing system, Medicaid eligibility and claims platform, unemployment-insurance system, or wildlife licensing and draw system is not interchangeable in the way that commodity office technology is. These systems are mission technology and require close agency ownership.

3. Four Technology Classes Require Different Governance

Technology class	Examples	Primary value	Default governance
Commodity services	Email, productivity, connectivity, standard endpoints, routine infrastructure	Scale, price, standardization	Standardize, aggregate demand, consolidate where economical
Enterprise platforms	IAM, cybersecurity tooling, workflow/BPM, document/content management, integration/API services, common collaboration, and statewide platforms such as SHARE ERP	Interoperability, reuse, security, portability, consistency	Enterprise-first/shared, with justified exceptions
Enterprise governance	Architecture, cybersecurity policy, data governance, portfolio/investment management, technology standards	Statewide risk management, accountability, investment discipline	Statewide authority and visibility
Mission technology	Medicaid, taxation, wildlife licensing/draw, corrections, unemployment insurance	Mission knowledge, statutory fidelity, program effectiveness	Agency ownership within enterprise guardrails

This distinction is consistent with shared-services evidence. The U.S. Government Accountability Office (GAO) found operational efficiencies and cost savings across all eight agencies it examined, cybersecurity benefits at seven of eight, and improved service delivery at most. The same study also documented legitimate operational, legal, integration, and legacy-system challenges. The implication is enterprise-first, not enterprise-only. **[S3, S4]**

4. Enterprise Platforms Create Value Beyond Procurement Savings

A statewide contract can lower the purchase price of technology. That is useful, but it is not the same as enterprise transformation. The larger opportunity comes when common platforms allow agencies to work together using common identities, controls, integration patterns, process conventions, and data exchanges.

New Mexico already has a major example: the Statewide Human Resources, Accounting and Management Reporting (SHARE) system is the State's enterprise resource planning (ERP) platform for financial and human-resource functions. The Department of Finance and Administration (DFA) manages the statewide PeopleSoft environment; official state sources describe SHARE as supporting financial and human-resource operations across state government. SHARE illustrates the distinction between an enterprise platform and agency mission systems: agencies retain their missions while common administrative processes operate on shared statewide infrastructure. **[S17]**

Identity and access management

Identity and access management (IAM) is foundational infrastructure for modern cybersecurity and digital service delivery. The National Institute of Standards and Technology (NIST) Zero Trust guidance treats identity, credentials, access management, and enterprise-wide access policy as core mechanisms for securing distributed enterprise resources. New Mexico's Microsoft Digital Workspace already demonstrates the enterprise pattern by providing a single State of New Mexico identity for participating workforce services. **[S5, S9]**

The same architectural principle can be extended to constituents. A statewide constituent identity capability could provide single sign-on across participating state websites and portals so that a person can authenticate once, access authorized personal information, and conduct transactions with multiple agencies without creating and maintaining a separate identity for every service. Agency systems would continue to determine what that person is authorized to see or do; the enterprise capability would provide trusted identity, authentication, and common access mechanisms.

Workflow, process management, and document control

Workflow and content-management platforms are especially important because their value can increase with common adoption. A common platform can provide reusable integrations, consistent approvals, process ownership, controlled procedures, audit trails, status visibility, escalation, and performance measurement across organizational boundaries. GAO found that shared services can standardize processes, reuse integrations, reduce administrative burden, and align business processes and data across functional areas. **[S3]**

The policy objective should not be to force every agency into one product regardless of mission needs. It should be to establish an enterprise workflow and process-management capability as the default for common and cross-agency processes, with interoperability standards and a transparent exception process.

5. Government Services Cross Agency Boundaries

Citizens experience government as a service, not as an organization chart. Responsibility for a single life event can move from one department to another, and many people receive related services from multiple agencies at the same time. The technology and operating model should therefore support both sequential handoffs and simultaneous cross-agency workflows, data exchange, status visibility, and accountability even when different agencies own different portions of the service.

A long-standing New Mexico example is the transition of certain young people from children's services to adult services. In 2001, the Legislature formally recognized the risk created when specialized foster-care services ended at age eighteen and called on CYFD, the Human Services Department, and the Department of Health to ensure an uninterrupted transition. More recent

legislation again directs CYFD and the Health Care Authority to collaborate in delivering services to children and families. **[S11, S12]**

Practitioner observations suggests that some cross-agency transitions can still operate as handoffs rather than as jointly managed processes. Those observations should not be presented as a verified statewide fact without additional documentation. It does, however, illustrate the design problem: an effective enterprise process should confirm receipt, assign responsibility, track exceptions, make status visible, and verify completion rather than merely transfer a package from one organization to another.

> **Agency A initiates → required information assembled → Agency B acknowledges receipt → case assigned → eligibility/service action completed → exceptions resolved → completion confirmed**

The principle is simple: **agencies own their portion of the business process; the enterprise can provide the machinery that allows the entire process to operate as one accountable service.**

6. New Mexico Already Has an Enterprise Foundation

The recommended direction is evolutionary, not a wholesale organizational reset. The Department of Information Technology (DoIT) Act was enacted in 2007 to consolidate duplicated enterprise technology services and charged the state CIO with reducing redundancy, improving interoperability and data accessibility, and recommending solutions when agency systems overlap or duplicate. Although the statute has been amended, its core governance design is now nearly two decades old. During that period, cloud computing, software-as-a-service, mobile government, Zero Trust security, application programming interfaces, digital identity, data platforms, and artificial intelligence have materially changed both technology and its importance to government operations. The next administration should therefore treat statutory modernization as part of the roadmap rather than assume a 2007 governance framework fully addresses the technology environment of 2027 and beyond. **[S6]**

Today, DoIT describes itself as the State's enterprise technology partner and says its Enterprise Services program exists to consolidate services previously duplicated within agencies. Current rules address enterprise architecture, electronic authentication, application software selection, project certification, and information-security operations. **[S7, S8]**

Recent enterprise delivery: DoIT announced the September 22, 2026 launch of a statewide ServiceNow service-management platform. Its announcement describes an approximately eight-week implementation and anticipated support for roughly 30–40 partner agencies. This is an example of a shared platform already being deployed; the announcement does not establish full statewide adoption, realized savings, or the completeness of enterprise governance. [S32]

Operationally, DoIT already functions in part as an internal managed service provider (MSP) for state agencies. Its catalog includes managed desktop, enterprise support desk, email and collaboration, application maintenance and development, file and print, networking, hosting,

storage, server administration, voice, and related services. This demonstrates that enterprise delivery is not a new concept for New Mexico; the policy question is which additional capabilities should become enterprise defaults and how service quality, accountability, and agency choice should be governed. A current authoritative public count of agencies receiving full managed-desktop/MSP-style support has not yet been identified, but it is estimated to be between one and two dozen such agencies. **[S7, S9, S16]**

In 2026, New Mexico also expanded statutory replacement planning to include software used to provide DoIT enterprise services, requiring annual equipment-and-software replacement plans for each enterprise function. That law is modest in scope, but it reinforces the principle that enterprise technology must be managed over its lifecycle, not merely purchased as a one-time commodity. **[S10]**

7. Five-Year Direction: Move Materially Along the Spectrum

New Mexico does not need to fully centralize state IT to achieve substantial gains. A practical goal is to move common capabilities materially toward the enterprise side of the spectrum during the next administration and reach a mature hybrid model within approximately five years.

Period	Primary objective	Illustrative actions
Transition / first 100 days	Establish direction and decision rights	Confirm enterprise governance; baseline capabilities; inventory major systems and investments; identify common-platform opportunities; define exception principles.
2027	Build enterprise foundations	Enterprise IAM strategy; architecture and cloud guardrails; data governance; portfolio/investment model; cybersecurity baseline; select 2–3 cross-agency process pilots.
2028	Deploy and prove shared capabilities	Implement priority enterprise platforms; demonstrate measurable workflow/data-sharing improvements; establish reusable integration patterns.
2029–2030	Scale and rationalize	Expand successful shared platforms; reduce duplicative capabilities; align procurement with architecture; improve constituent identity and cross-agency service delivery.
2031	Institutionalize the operating model	Measure outcomes; complete major migrations; update statutes/rules where required; publish the next statewide technology plan.

8. Priority Enterprise Capabilities

1. Identity and access management. A common workforce identity and access model, plus a constituent identity strategy that can support single sign-on across participating state websites and portals while preserving agency-specific authorization and privacy controls.

2. Cybersecurity. Statewide policy, monitoring, incident response, shared tooling, and common security baselines proportional to risk.

3. Data governance and interoperability. Common definitions, stewardship, exchange patterns, and lawful mechanisms for moving data when service delivery crosses agency boundaries.

4. Enterprise architecture and enabling platforms. Architecture guardrails plus shared capabilities such as workflow/BPM, document/content management, integration/API services, and common cloud foundations where enterprise delivery creates value.

5. Portfolio and investment governance. Statewide visibility into major systems, lifecycle risk, technical debt, duplication, dependencies, and technology investment decisions.

6. Major-project delivery reform. Establish accountable agency product owners, credible baseline and forecast reporting, incremental demonstrations of working capabilities, modular contracting where appropriate, and independent checkpoints on vendor outcomes. Technology/project approval should remain distinct from procurement execution under the 2025 statutory framework. [S20, S31]

9. Organization and Accountability Must Also Evolve

- The roadmap does not require an immediate wholesale transfer of all agency IT employees to DoIT. It should, however, evaluate selective personnel consolidation where statewide delivery would improve capability, security, career paths, staffing resilience, or accountability.
- Agency chief information officers (CIOs) and IT directors should have a formal functional relationship to the State CIO even when they continue to report administratively to their agency secretaries. A dotted-line or equivalent governance relationship could establish common expectations for architecture, cybersecurity, workforce planning, professional standards, and enterprise initiatives without removing agency accountability for mission delivery. **[S18]**
- Selective consolidation should preserve agency ownership of statutes, programs, business rules, product priorities, and mission outcomes. The State CIO organization should own or govern enterprise concerns; agency leadership should remain accountable for mission results.
- This is not unprecedented in New Mexico. The 2007 consolidation initiative contemplated IT staff consolidation as one component of enterprise reform, alongside shared business functions such as SHARE and technical-services consolidation such as networks, email, security, identity management, and data centers. A 2010 Legislative Finance Committee review still described staff consolidation as part of the state's consolidation model. **[S16]**
- The exact reporting model should be designed deliberately. NASCIO research finds no single prevalent state model for agency-CIO reporting relationships; states range from fully centralized reporting to no formal reporting relationship. NASCIO identifies governance strength and relationships among state and agency technology organizations as the more important common factor. New Mexico should therefore choose and

codify a model that creates real enterprise accountability rather than assume organizational structure alone will produce it. **[S18]**

Conclusion

The central choice for New Mexico is not federation or consolidation in the abstract. It is whether the State will continue allowing common capabilities to evolve primarily as separate agency decisions, or deliberately manage those capabilities as statewide assets.

> **Commodity technology should exploit statewide scale. Enterprise platforms should be shared where common adoption creates interoperability, security, portability, consistency, or efficiency. Enterprise-wide risks and investments should be governed statewide. Mission technology should remain close to the agencies that understand the programs it implements.**

That approach offers a practical path for moving New Mexico materially along the governance spectrum within five years while preserving the mission ownership, program accountability, and specialized capabilities that belong with individual agencies.