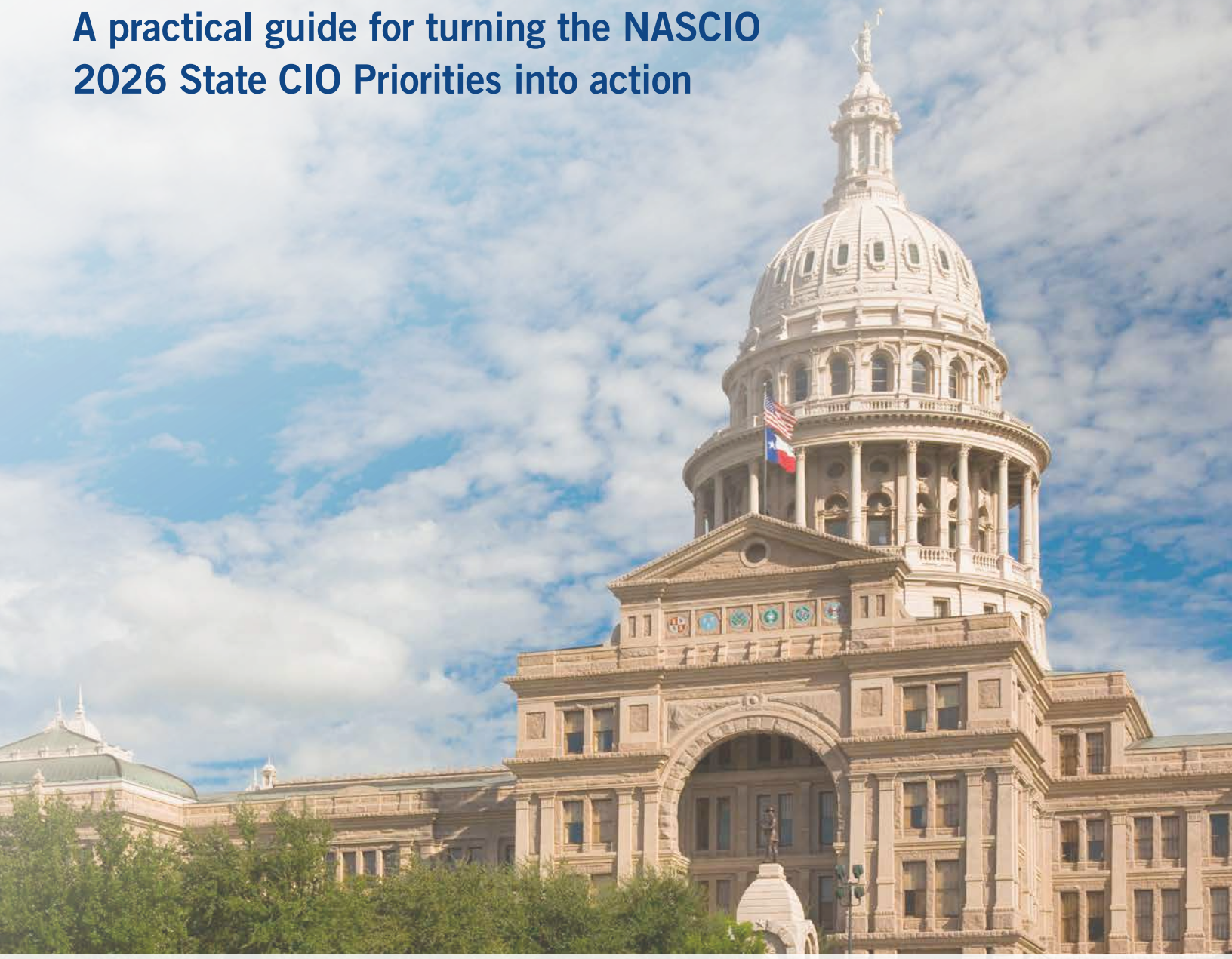
STATE CIO 2026 PRIORITIES PLAYBOOK

A practical guide for turning the NASCIO 2026 State CIO Priorities into action



Russell Gainford, Chief Technology Officer, Tyler Technologies

Liz Thomas, President, State & Federal Group, Tyler Technologies

tyler technologies

Introduction

For the 20th year, the National Association of State Chief Information Officers (NASCIO) has published its State CIO Top 10 Priorities[1], offering a clear view of how state technology leaders are responding to evolving demands. The 2026 priorities reflect both continuity and change: artificial intelligence rises to the top for the first time, cybersecurity remains foundational, and attention continues to focus on accessibility, cost pressures, and optimization.

Most state CIOs are already familiar with this list. The harder question is what it means in practice — how these priorities show up in day-to-day decisions, how they intersect, and how agencies sequence progress without overextending people, budgets, or systems.

This playbook is designed to support that next step. Drawing on Tyler Technologies' experience working alongside state governments nationwide, it pairs practical recommendations with real-world examples from agencies making measurable progress. The goal is not to prescribe a single path forward, but to provide clear, grounded insight leaders can adapt to their own context.

The sections that follow explore each priority in turn, focusing on what matters now — and what to prepare for next.

[1] National Association of State Chief Information Officers. (2025, December 15). *State CIO Top Ten Policy and Technology Priorities for 2026.* https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2026/

2026 State CIO Top 10 Priorities

Click on a priority title to jump to that page.

Priority 1: Artificial Intelligence / GenAI / Agentic AI / Machine Learning

The Issue

Artificial intelligence (AI) has captured enormous attention, but for state CIOs its value is grounded in practical need. Agencies face pressure to improve service delivery, support a stretched workforce, and make better use of data — often without increases in budget or staffing. AI is increasingly seen as a way to extend capacity: reducing repetitive work, strengthening decision-making, and helping residents find and complete what they need more easily. As a result, states are moving beyond pilots and applying AI to real, measurable challenges. Doing so responsibly requires governance that ensures AI can be used confidently in everyday operations.

Why Progress Stalls in Practice

AI adoption in government is constrained by several realities. It is only as reliable as the data behind it, and many agencies are still working through fragmented systems, inconsistent standards, and unclear ownership. Leaders must also balance innovation with transparency, security, and public trust, while introducing new capabilities without disrupting essential services or overwhelming staff. Progress requires careful sequencing, not acceleration for its own sake.

What Leaders Should Do Differently

Leaders need to apply the same deliberate approach used in other modernization efforts. They define outcomes first, prioritize use cases, and establish clear ownership before scaling solutions. Strong data foundations remain essential, but they are treated as part of a broader governance model that guides how teams access, use, and trust information. These efforts return time to staff, strengthen decision-making, and help residents find what they need more quickly — not by replacing people, but by supporting the mission of public service.

What to Prioritize First: AI Governance

AI governance has always depended on strong data practices, but it extends beyond data alone. As governments prepare for more advanced capabilities — including agentic AI — clear oversight, defined accountability, and trusted data together form the foundation that allows AI use to scale with confidence and purpose.

Case Study

In South Carolina, an AI-based resident assistant lets residents ask questions in their own words and get quick, conversational answers. It helps users complete tasks like applying to be a notary or paying taxes and is answering more than 4,000 questions per month with 72% user satisfaction, a strong result for a public-sector digital service. In 2026, South Carolina is rolling out an additional solution that will use robust AI models to verify the identity of individuals when performing secure online transactions with agency services.

Further Reading

E-Book: AI for Impact - Proven Results for Government

Supporting Tyler Solutions

Artificial Intelligence Solutions for the Public Sector

Augmented Field Operations

Resident AI Assistant

RECOMMENDED STEPS: AI GOVERNANCE

1 — PRIORITIZE WHAT MATTERS
Focus on low-risk, high-impact use cases to address needs and build trust.

2 — BUILD A TRUSTED DATA FOUNDATION
Govern the data and content AI relies on.

3 — LEAD WITH OVERSIGHT
Ensure executive and expert review.

4 — PREPARE THE WORKFORCE
Set expectations and build confidence.

5 — EVALUATE AND IMPROVE
Monitor performance and refine over time.

Priority 2: Cybersecurity & Risk Management

The Issue

Cybersecurity has consistently been among the top priorities of state CIOs for many years. Agencies recognize that security is no longer a discrete function or a technical checklist. It is a governance responsibility that spans budgets, procurement, data stewardship, and workforce readiness. That challenge is compounded as bad actors increasingly use artificial intelligence to make attacks easier to launch, faster to scale, and harder to detect. The emphasis on whole-of-state cybersecurity reflects a shared reality across states: risk rarely respects organizational boundaries, and neither can the response.

Why Progress Stalls in Practice

Progress stalls on several fronts. Security expectations continue to rise while budgets, staffing, and institutional authority often lag behind. CIOs are expected to manage increasingly complex risks — from insider threats to third-party exposure — using fragmented tools, uneven training, and governance models not designed for shared accountability. The challenge is less about awareness and more about alignment: Who owns risk decisions, how tradeoffs are made, and how resilience is sustained as conditions change.

What Leaders Should Do Differently

Reframing cybersecurity as part of operational resilience, rather than a standalone defense effort, is critical for progress. Agencies that succeed treat data protection, security frameworks, and workforce awareness as reinforcing systems, not parallel initiatives. Risk management becomes an ongoing discipline embedded in how technology investments are prioritized, how vendors are evaluated, and how continuity is planned — recognizing that disruption can originate from cyber incidents, infrastructure failures, or external dependencies.

What to Prioritize First: Resilience

This perspective shifts the conversation from preventing every incident to being prepared for whatever comes next. Building resilience requires deliberate alignment between governance, technology, and people, with a clear understanding of shared risk across the enterprise. The steps that follow focus on how agencies translate this mindset into durable practices that support continuity, adaptability, and public trust over time.

Further Reading

E-Book: Resilient by Design: How Technology Supports Government

Supporting Tyler Solutions

Cybersecurity

RECOMMENDED STEPS: BUILDING A FOUNDATION FOR RESILIENCE

1 — IDENTIFY CRITICAL SERVICES

What's most disruptive to operations and residents if it fails?

2 — EVALUATE RISKS AND INTERDEPENDENCIES

Examine how critical services are connected to other systems.

3 — PLAN IN PHASES

Start with services that need to be always on. Build a phased roadmap.

4 — TEST AND PRACTICE

Run quarterly drills and exercises. Verify documents. Use sample sizing.

5 — ALIGN WITH MODERNIZATION

Modernization and resilience aren't separate initiatives. They're linked.

6 — EMBED WITH OPERATIONS

Make resilience part of your budgeting and operations.

Priority 3: Budget / Cost Control / Fiscal Management

Case Study

A large western state used an AI-enhanced solution to benchmark every program in five of their agencies against peer organizations and identify cost savings, alternative revenue, and consolidation opportunities. They identified $164M–$225M in annual opportunity, backed by division-level findings, peer-state case studies, and specific implementation pathways tailored to the state's funding structure and scale.

Further Reading

White Paper: Reframe Uncertainty With Priority Based Budgeting

Supporting Tyler Solutions

Priority Based Budgeting

The Issue

State CIOs are under growing pressure to control costs while sustaining service levels and advancing strategic priorities. Traditional budgeting approaches, built around line items and incremental adjustments, make it difficult to see how spending aligns with outcomes or to respond flexibly when conditions change. As fiscal uncertainty persists, leaders are looking for ways to move beyond across-the-board cuts or short-term fixes and instead make deliberate, defensible decisions about where resources create the most value.

Why Progress Stalls in Practice

Budgeting falters when it remains anchored to line items rather than outcomes. Traditional approaches make it difficult to see how resources align across programs, agencies, or enterprise priorities, especially when funding arrives through a mix of appropriations, one-time allocations, and chargeback models. In times of uncertainty, leaders can become locked into a false binary: raise taxes or cut services. That framing limits options, obscures tradeoffs, and reinforces short-term decisions that are misaligned with long-term needs.

What Leaders Should Do Differently

CIOs and budget leaders need to elevate budget conversations earlier and make them more strategic — shifting from defending expenditures to clarifying value. Priority-based budgeting supports this shift by linking spending to programs, populations served, mandates, and strategic goals, while still building on existing line-item structures. Rather than predicting outcomes in advance, leaders create a shared, data-informed view of how resources are currently allocated, enabling more confident decisions under constraint.

What to Prioritize First: Priority-Based Budgeting

Momentum starts by adopting priority-based budgeting to align fiscal discussions around programs and outcomes rather than accounts and categories. When leaders share a common view of what government is trying to achieve — and how resources currently support or hinder those priorities — budget decisions become less reactive and more intentional. This clarity creates the foundation for disciplined reallocation and sustained fiscal management under changing conditions.

RECOMMENDED STEPS: IMPLEMENTING PRIORITY-BASED BUDGETING

1 — START WITH LINE-ITEM DATA
Use existing line-item budget data as the foundation.

2 — INVENTORY PROGRAMS
Analyze existing budget data to create an inventory of programs.

3 — UNDERSTAND PROGRAM COSTS
Gain predictive insight into the actual costs of programs.

4 — SCORE PROGRAMS
Rank and prioritize programs according to resident impact.

5 — REALLOCATE RESOURCES
Redirect funding based on program-level insights.

Priority 4: Modernization

The Issue

Modernization remains a core priority for state CIOs because it supports nearly every other strategic objective — from cybersecurity and workforce sustainability to service reliability and cost control. Aging platforms and fragmented processes make it harder to adapt as demands increase. At the same time, modernization is no longer defined solely by wholesale replacement of systems. For many states, it means deliberately enhancing, renovating, or selectively replacing systems and workflows so they better support today's operational realities.

Why Progress Stalls in Practice

Despite broad agreement on the need, modernization often advances unevenly. Technical debt accumulates gradually and competes with more visible, immediate demands. Workforce transitions complicate timing, as agencies must support legacy knowledge while preparing for new skills and expectations. Security concerns raise urgency, yet fear of disruption can slow required action. These dynamics can leave agencies maintaining systems that are "good enough" in the short term but increasingly fragile over time.

What Leaders Should Do Differently

Anchoring modernization in business purpose rather than technology cycles can help sustain momentum. Instead of asking what should be replaced, agencies shift their focus to what outcomes matter most — risk reduction, operational resilience, and team capacity — and let those priorities shape modernization decisions. This framing positions technology as a means to strengthen the organization's footing, not as an end in itself.

What to Prioritize First: Outcome-Driven Modernization

Modernization efforts gain traction when they are aligned to concrete agency goals and pursued in a deliberate order. Security, workforce capacity, partner expertise, and budget reality all influence what should move first and what can wait. When leaders treat modernization as a sequence of intentional decisions — rather than a single migration or upgrade — they create room to reduce risk, build confidence, and sustain progress over time. This framing creates the conditions for staged action, rather than forcing premature or fragmented change.

Further Reading

E-Book: Cloud-Smart Strategies for IT Infrastructure Modernization

Supporting Tyler Solutions

Digital Titling

Augmented Field Operations

Resident Engagement Platform

Disbursements

RECOMMENDED STEPS: OUTCOME-DRIVEN MODERNIZATION

1 — MATCH MODERNIZATION TO GOALS
Define your top needs and technology projects that address them.

2 — MIGRATE FOR SECURITY
Prioritize cloud migrations that materially strengthen security posture.

3 — PARTNER FOR EXCELLENCE
Require expertise in both the public sector and cloud-based solutions.

4 — PROCEED IN STAGES
Multiyear plans accommodate budget and staffing constraints.

5 — BUILD MOMENTUM
Track metrics and share progress with team and community.

Priority 5: Digital Government / Digital Services

The Issue

For many states, digital government is now the primary way residents experience government. What once supplemented in-person or paper-based services is now the front door — shaping trust, accessibility, and satisfaction. CIOs are navigating rising expectations for seamless access, personalization, privacy, and security while also being asked to demonstrate measurable value. This priority is not about adding more portals or digitizing individual transactions. It is about creating a connected digital environment that enables consistent, secure, and meaningful engagement with residents across programs and agencies.

Why Progress Stalls in Practice

Progress slows when digital initiatives focus on channel expansion rather than engagement continuity. Agencies modernize individual services, but identity systems remain fragmented, notifications are disconnected, and residents must repeatedly reintroduce themselves across agencies. Cost-benefit discussions center on project delivery rather than long-term engagement outcomes. Meanwhile, accessibility mandates, privacy protections, and security requirements must be reconciled across systems that were never designed to work together. The result is incremental improvement without a cohesive resident relationship — progress that appears modern internally but remains fragmented externally.

What Leaders Should Do Differently

Leaders advancing this priority treat digital services as enterprise infrastructure for an ongoing relationship with residents. That means shifting from a program-by-program mindset to one that considers how identity, access, communication, and transactions work together over time. Governance conversations start with the resident journey and work backward to technology and policy implications. It also requires realism about funding cycles, workforce capacity, and statutory guardrails. From our work with states, durable progress occurs when digital modernization is framed not as technology transformation, but as infrastructure for sustained public engagement.

What to Prioritize First: Cohesive Resident Engagement

Momentum builds when states align identity, accessibility, privacy, security, and cross-agency governance around a shared model for resident engagement. Establishing that coherence early allows modernization efforts — including portals, payments, forms, notifications, and records — to reinforce a single, trusted digital relationship. This orientation ensures subsequent investments reinforce continuity rather than expand fragmentation.

Case Study

Vermont improved outdoor recreation services with a mobile-first platform that centralizes permits, regulations, reporting, and location-based information. The app reached nearly 5,000 downloads in its first week and continues to support compliance, public safety, and efficient service delivery — reducing friction for residents while freeing agency staff to focus on higher-value work across agencies.

Further Reading

E-Book: A Digital Guide to Modernizing the Resident Experience

Supporting Tyler Solutions

Outdoor Recreation

Payments

Digital Titling

Resident Engagement Platform

RECOMMENDED STEPS: COHESIVE RESIDENT ENGAGEMENT

1 — DEFINE RESIDENT NEEDS
Prioritize key resident needs and pain points.

2 — PLAN FOR DELIVERY
Secure necessary funding, resources, and partnerships.

3 — AUDIT POLICIES
Account for data security, privacy, and compliance needs.

4 — BUILD CHANGE READINESS
Adopt change management strategies and establish capacity-building and skill development initiatives.

5 — ASSESS IMPACT
Track user adoption, service usage, payments processed, user interactions, and other metrics.

Priority 6: Accessibility

The Issue

As society becomes increasingly reliant on digital platforms, the importance of accessible government services has become more apparent — and more urgent. For many residents, accessibility is not simply a legal requirement. It is essential for full participation: the ability to connect to essential services and benefit equally. When digital channels are the default doorway to government, barriers created by outdated systems, poorly designed platforms, or limited inclusivity do more than inconvenience people. They can exclude residents with disabilities and erode trust in government operations. Accessibility also carries rising compliance pressure, including DOJ rules, making it a priority states must address.

Why Progress Stalls in Practice

Obstacles that span both technical and organizational dimensions can impede progress. Governments may encounter challenges trying to incorporate accessibility into design and development in a way that continually improves outcomes for people with disabilities while also reducing legal liabilities. Training and funding gaps make it harder to build accessibility into everyday workflows. Fragmented and outdated systems — disconnected platforms that frustrate residents and staff — further limit consistency. And even when intent is clear, navigating compliance requirements that vary by entity adds complexity that can slow decisions and dilute accountability.

What Leaders Should Do Differently

Leaders need to treat accessibility as a core part of digital access and resident experience. The practical emphasis is inclusive design from the outset: understanding the needs of diverse users, anticipating barriers early, and using research, feedback, and audits to guide improvements. Modernization choices matter here as well. When states move away from disconnected legacy environments toward more adaptable platforms, accessibility becomes easier to embed and sustain rather than patched in after the fact.

What to Prioritize First: Inclusive Design

What differentiates accessibility efforts that last is an emphasis on inclusive design — recognizing existing commitments while balancing planning, collaboration, and iterative improvement. Comprehensive audits help clarify what may need to change over time. Resident engagement and focus groups ensure solutions reflect real-world needs and lived experiences. Pilots create space to learn and refine before scaling. Careful resource allocation helps teams navigate familiar constraints like budget limits and system integration. Taken together, this approach grounds the practical considerations and keeps accessibility work rooted in detail, progress, and partnership.

Case Study

Indiana's Office of Technology offers free IN.gov website hosting to local governments, providing 508-compliant adaptive templates, IN.gov subdomains, and a no-code CMS. By removing financial barriers and centralizing hosting, the program empowers small towns and large communities to improve accessibility, security, and resident access. Over 100 governments enrolled, receiving migration, training, and ongoing support to deliver inclusive digital services.

Further Reading

E-Book: Digital Access and Accessibility in the Resident Experience

Supporting Tyler Solutions

Resident Engagement Platform

RECOMMENDED STEPS: INCLUSIVE DESIGN

1 — CONDUCT ACCESSIBILITY AUDITS
Identify gaps and prioritize improvements.

2 — ENGAGE THE PUBLIC
Ensure systems address real-world needs.

3 — RUN PILOT PROGRAMS
Refine solutions before scaling.

4 — ALLOCATE RESOURCES DELIBERATELY
Address budget constraints and integration challenges.

5 — PARTNER WITH ACCESSIBILITY EXPERTS
Add expertise and tools tailored to the public sector.

Priority 7: Identity & Access Management

The Issue

Identity and access management (IAM) is fundamental to how states deliver digital services. As residents and businesses increasingly expect government interactions to mirror the convenience of online banking or e-commerce, states are rethinking how identity works across agencies. In concept, this priority is about establishing a centralized digital identity that allows individuals to authenticate once and interact seamlessly across multiple services. But the ambition extends beyond single sign-on. States are working toward comprehensive user profiles that reflect a person's relationship with government, enabling faster transactions, fewer repetitive forms, and more consistent experiences across programs.

Why Progress Stalls in Practice

Identity initiatives may inherit the fragmentation they are meant to solve. Legacy systems, agency-specific data ownership, and uneven technology maturity complicate efforts to centralize authentication and access control. Many states still operate with early-stage IAM approaches focused on basic authentication and authorization, with limited interoperability between services. As states introduce stronger security measures like multi-factor authentication, role-based access controls, and single sign-on, they sometimes find that coordination across departments and systems becomes the constraint — especially as public-facing identity needs scale beyond the back office.

What Leaders Should Do Differently

Leaders need to treat identity as shared digital infrastructure. They align identity decisions to both internal workforce access and resident-facing services, with consistent standards for authentication, credentialing, and access control. They also balance usability with accessibility, security, and privacy — recognizing that systems must be intuitive for the public, resilient under high demand, and designed to protect user information. Prioritizing interoperability helps identity function across agencies and applications, while scalability ensures the approach can expand as services and user volumes grow.

What to Prioritize First: Shared Identity Infrastructure

As states move beyond early IAM implementations, the first priority is establishing shared identity infrastructure that works across agencies and services. Addressing change management questions across technical, financial, and organizational functions helps ease adoption, while tracking public experience metrics provides insight into how identity services are performing in practice. Together, these efforts create the foundation for scalable, trusted identity systems that support both workforce access and resident-facing services.

Case Study

The Indiana Office of Technology wanted to make the state's sprawling digital assets — including 626 websites, 100,000 pages of content and more than a million digital assets across 100 state agencies — more navigable for residents. They partnered with Tyler to provide single sign-on capabilities, creating unified access to more than 175 applications for 2.9 million users.

Further Reading

White Paper: Improving Resident Engagement With Identity and Access Management

Supporting Tyler Solutions

Resident Engagement Platform

RECOMMENDED STEPS: BUILDING SHARED IDENTITY INFRASTRUCTURE

1 — ALIGN IDENTITY ACROSS AGENCIES
Establish shared standards for authentication, credentialing, and access control.

2 — PLAN FOR CHANGE MANAGEMENT
Address technical, financial, and organizational impacts early to support adoption.

3 — DESIGN FOR PUBLIC EXPERIENCE
Prioritize ease of use, accessibility, and clarity for residents and businesses.

4 — MEASURE ADOPTION AND PERFORMANCE
Track usage, response times, and system reliability to guide improvement.

5 — BUILD TRUST THROUGH SECURITY AND PRIVACY
Reinforce confidence by protecting data and monitoring security outcomes.

Priority 8: Data Management & Analytics

The Issue

Data management and analytics are essential to how many state agencies plan, operate, and deliver services. While government has always relied on information, the scale and complexity of today's data environment are fundamentally different. Cloud platforms and advanced analytics have made it possible to aggregate information across programs and agencies in ways that were previously out of reach. The pandemic accelerated this shift, demonstrating how timely, integrated data can inform decisions, improve service delivery, and build public trust. As expectations rise for transparency, efficiency, and insight, leaders recognize that data is not a back-office asset — it is a strategic capability that underpins nearly every CIO priority.

Why Progress Stalls in Practice

Even with broad agreement on data's value, many states struggle to translate volume into insight. Data may be fragmented across systems, managed inconsistently, and shared informally. Agencies sometimes invest in analytics tools without first establishing common standards for data quality, access, and security. Roles and responsibilities for data stewardship are frequently unclear, leaving governance dependent on goodwill rather than accountability. The result is an environment where leaders have more data than ever, but may lack confidence in its accuracy, completeness, or appropriate use — especially as predictive analytics and AI place higher demands on data integrity.

What Leaders Should Do Differently

Leaders need to treat data strategy as an organizational discipline. They anchor analytics, business intelligence, and data architecture decisions in shared expectations about how data will be governed, protected, and used. Strong executive leadership commitment, clear communication of data's purpose, and sustained attention to change management help agencies move from ad hoc data use toward consistent, repeatable practices that support collaboration and informed decision-making.

What to Prioritize First: Data Governance Foundations

Effective data governance provides the structure that makes advanced analytics possible. Clarifying why data matters, understanding what data exists, enabling unified access, improving quality, and assigning clear ownership create trust in the information leaders rely on. Following these steps ensures that investments in dashboards, predictive models, and AI rest on data that is reliable, secure, and fit for purpose — setting the stage for more sophisticated use over time.

Case Study

The Massachusetts Office of the Comptroller wanted to change how the state's leaders and constituents viewed the role of open data in government. Using Tyler solutions, they provide visuals of data — such as health and human services costs, expenditures, and payroll data — so residents, journalists, and staff can more easily understand and use information to support transparency, oversight, and informed decision-making.

Further Reading

E-Book: A Digital Government Guide to Effective Data Strategies

Supporting Tyler Solutions

Data & Insights

RECOMMENDED STEPS: DATA GOVERNANCE FOUNDATIONS

1 — DEFINE OUTCOMES
What decisions or services will better data enable?

2 — INVENTORY YOUR DATA
Identify what you have, where it lives, and who owns it.

3 — UNIFY ACCESS
Create shared platforms and metadata standards.

4 — CLEAN AND STANDARDIZE
Correct errors, align formats, and remove duplicates.

5 — ASSIGN OWNERSHIP
Designate data stewards to maintain quality and monitor use.

Priority 9: Consolidation / Optimization

The Issue

Consolidation and optimization are rising priorities as state CIOs contend with environments shaped by years of incremental growth. Agencies often operate overlapping systems and parallel processes that perform similar functions, increasing cost, complexity, and operational risk. As workforce capacity tightens and expectations for reliability rise, this fragmentation limits agility. Today, consolidation is about simplifying how government operates by reducing duplication, standardizing workflows, and enabling systems to work together without ongoing customization as demands change.

Why Progress Stalls in Practice

Consolidation efforts often stall because they disrupt established ownership models and funding structures. Systems are deeply embedded in agency operations, incentives favor local control over enterprise efficiency, and migration efforts create fear of service disruption. Data dependencies and unclear governance further complicate decisions. Without a shared definition of value and clear authority to act, agencies frequently maintain parallel systems even when the long-term operational cost is widely understood.

What Leaders Should Do Differently

Leaders need to approach consolidation as an operational strategy rather than a cost-cutting mandate. They should focus first on simplifying high-volume, high-effort processes and standardizing workflows before pursuing deeper system consolidation. AI-enabled document automation can play a key role by reducing manual intake, routing, and data entry across these workflows. Successful CIOs align agencies around shared outcomes such as speed, consistency, and capacity. By pairing consolidation with process optimization and clear governance, they reduce complexity while improving reliability and resilience across the enterprise.

What to Prioritize First: Standardized Workflows

The fastest gains from consolidation often come from standardizing how work is performed, not from replacing every system at once. Establishing common intake, review, and processing workflows across agencies reduces duplication and exposes opportunities to retire or merge systems over time. This approach lowers risk, delivers visible improvements early, and creates a practical foundation for deeper consolidation driven by performance and sustainability rather than mandate.

Case Study

Montana consolidated paper-based and decentralized property assessment filings by moving high-volume submissions to a centralized digital workflow. The shift reduced duplication across 31 field offices, cut statewide postage costs by approximately $100,000, and significantly reduced manual data entry. By standardizing intake and review, the state improved processing speed and scaled operations more effectively during periods of increased demand.

Supporting Tyler Solutions

Document Automation

SmartFile

Digital Titling

Augmented Field Operations

Resident AI Assistant

Vitals Access

RECOMMENDED STEPS: STANDARDIZING AND OPTIMIZING OPERATIONS

1 — IDENTIFY HIGH-VOLUME PROCESSES

Focus on workflows that consume the most staff time or generate repeated effort across agencies.

2 — MAP AND COMPARE WORKFLOWS

Document how similar work is performed today to surface redundancy and variation.

3 — STANDARDIZE INTAKE AND REVIEW

Establish common processes that reduce manual handling and routing complexity.

4 — CENTRALIZE WHERE IT ADDS VALUE

Consolidate processing or systems when it improves consistency, speed, and efficiency.

5 — RETIRE REDUNDANCY AND GOVERN FOR SUSTAINABILITY

Decommission duplicate tools and maintain oversight to prevent sprawl from returning.

Priority 10: Cloud Services

The Issue

As cloud-based solutions become the default delivery model for many state agencies, CIOs are shifting from a simple mandate to "move to the cloud" toward a more disciplined effort to operate effectively within it. This priority reflects a broader recognition that cloud strategy now supports modernization, security, service delivery, and innovation across government. Instead of concentrating narrowly on infrastructure replacement, leaders are focused on how cloud deployment models, governance, procurement, and service management work together to support scalable, resilient operations over time.

Why Progress Stalls in Practice

Despite widespread adoption, agencies sometimes struggle to realize the full value of the cloud. Cost concerns often dominate early conversations, especially when cloud subscriptions are compared to familiar on-premises expenditures. At the same time, technical debt from legacy systems, fragmented hybrid environments, and isolated cloud tools increase complexity and produce friction that slows progress. Workforce constraints further complicate the picture, as agencies balance day-to-day operations with the skills and planning required to manage cloud environments effectively. Without a cohesive, enterprise-level approach, cloud adoption can unintentionally introduce new silos rather than reduce them.

What Leaders Should Do Differently

Leaders need to reframe cloud adoption as a long-term operating model. They evaluate total cost of ownership, not just upfront price, and recognize how automated updates, centralized security, and elastic scalability reduce operational burden over time. Leaders are also prioritizing architectural coherence — sequencing migrations thoughtfully, reducing technical debt, and ensuring new systems are designed to work together. In this context, the cloud becomes an enabler of interoperability, faster iteration, and readiness for emerging capabilities such as AI.

What to Prioritize First: Cloud as an Operating Model

As with many of the other priorities, a pragmatic and detail-oriented approach is best. Before accelerating migrations, states should focus on readiness and alignment. Taking inventory of current systems, identifying high-impact priorities, and sequencing transitions strategically creates momentum while minimizing disruption. Building feedback loops and engaging experienced partners helps agencies adapt as they go. This measured approach establishes the foundation needed to live — and succeed — in the cloud.

Case Study

The North Carolina Administrative Office of the Courts migrated to Tyler's cloud-based solutions to create a paperless, interconnected case management system available 24/7. The agency has saved over 4 million sheets of paper while accepting more than 1.3 million electronic filings and handles a monthly load of more than 1.5 million online searches.

Further Reading

E-Book: Modern Governments Live in the Cloud

Supporting Tyler Solutions

Cloud Infrastructure for Government

RECOMMENDED STEPS: OPERATING EFFECTIVELY IN THE CLOUD

1 — ASSESS READINESS AND DEFINE
Inventory systems and data; set modernization objectives.

2 — IDENTIFY PRIORITIES
Start where pain is greatest to create early value.

3 — SEQUENCE STRATEGICALLY
Plan interdependencies to maintain continuity.

4 — MINIMIZE DISRUPTION
Align to budgets, peak workloads, and service windows.

5 — BUILD IN FEEDBACK LOOPS
Gather input at each phase to refine the plan.

6 — PARTNER WITH EXPERTS
Leverage provider and peer know-how tailored to government.

A Look Ahead

Taken as a whole, the NASCIO 2026 State CIO Top 10 Priorities underscore a defining reality for state technology leaders: Making progress requires understanding how they interact. Artificial intelligence, cybersecurity, data management, cloud services, accessibility, digital government, and modernization are distinct areas of focus, but in practice they are deeply connected. Decisions made on one priority inevitably shape outcomes in others.

As this playbook has shown, success pursuing these priorities does not reliably flow from isolated initiatives. Agencies achieve more sustainable progress by paying close attention to sequencing — strengthening data foundations before applying advanced analytics, aligning identity and accessibility efforts with digital services, and treating security as a shared operational responsibility rather than a standalone function. Across priorities, leadership engagement and organizational alignment emerge as enablers, particularly where change affects workflows, roles, and public expectations.

At the same time, agencies are navigating real constraints. Legacy systems, workforce capacity, regulatory obligations, and budget realities shape what is possible and when. Progress looks different for every organization. That variation is not a weakness; it reflects the complexity of governing at scale.

Thankfully, the path forward does not require solving everything at once. Practical progress comes from assessing what matters most, starting with achievable steps, and building from there. Incremental improvements, phased adoption, and sustained attention to execution allow agencies to manage risk while maintaining momentum. Viewed this way, pursuit of these priorities is not a race to an endpoint, but a continuous journey — one that rewards clarity, discipline, and steady leadership in service of better outcomes for the public.

Acknowledgments

Tyler Technologies thanks the National Association of State Chief Information Officers (NASCIO) for producing the annual State CIO Top 10 Priorities and for its ongoing work to advance government excellence through collaboration, shared best practices, and technology leadership.

Tyler is a corporate member of NASCIO.

Further Reading

Artificial Intelligence / GenAI / Agentic AI / Machine Learning
E-Book: AI for Impact – Proven Results for Government
White Paper: Revolutionizing the Government Workforce With AI

Cybersecurity & Risk Management
E-Book: Resilient by Design: How Technology Supports Government
Issue Paper: Strategies for Fraud Monitoring and Prevention

Budget / Cost Control / Fiscal Management
White Paper: Reframe Uncertainty With Priority Based Budgeting

Modernization
E-Book: Cloud-Smart Strategies for IT Infrastructure Modernization

Digital Government / Digital Services
E-Book: A Digital Guide to Modernizing the Resident Experience
Industry Insight: How to Increase Community Engagement

Accessibility
E-Book: Digital Access and Accessibility in the Resident Experience
White Paper: Indiana's Path From Digital Sprawl to Seamless Service

Identity & Access Management
White Paper: Improving Resident Engagement With Identity and Access Management
Issue Paper: The Case for Centralized Digital Identities

Data Management & Analytics
E-Book: A Digital Government Guide to Effective Data Strategies

Cloud Services
E-Book: Modern Governments Live in the Cloud
Industry Insight: AWS GovCloud (US) vs. AWS Standard (US)

Additional Resources

To learn more about our solutions for state agencies, visit Serving States on tylertech.com.

About the Authors

Russell Gainford is the chief technology officer at Tyler Technologies, where he leads cloud development, operations, and deployment strategy. His work helps public sector agencies deliver secure, scalable services through modern cloud infrastructure.

Liz Thomas is president of Tyler's State & Federal Group, where she leads teams delivering practical, results-driven innovation. Her work focuses on helping governments operate more effectively and realize greater value from their technology.

About Tyler's Solutions

Tyler Technologies delivers platforms and solutions to state governments proven to increase efficiencies, reduce costs, and serve residents more effectively. Backed by decades of experience and a deep understanding of government, our technology and tailored services solve real-world challenges and focus on long-lasting solutions.

From digital identities and payments to data-driven insights and AI, our wide range of secure, scalable solutions drive more effective government and enhance resident experiences. With capital city teams embedded across the country, we build long-standing partnerships with states so that they make the most of their investments.

As state governments continue to migrate to the cloud, our strategic collaboration with Amazon Web Services (AWS) positions us to leverage the cloud to deliver a better experience for our users and constituents while reducing costs and increasing efficiency and security. More than 14,200 clients use Tyler's cloud-based solutions.

Our commitment to state government is simple: deliver practical, results-driven innovation through systems that work so governments can focus on what matters most.

CONTACT TYLER

If you would like more information about Tyler solutions, contact us at info@tylertech.com or visit tylertech.com.

About Tyler Technologies, Inc.

Tyler Technologies (NYSE: TYL) is a leading provider of integrated software and technology services for the public sector. Tyler's end-to-end solutions empower local, state, and federal government entities to operate efficiently and transparently with residents and each other. By connecting data and processes across disparate systems, Tyler's solutions transform how clients turn actionable insights into opportunities and solutions for their communities. Tyler has more than 45,000 successful installations across 15,000 locations, with clients in all 50 states, Canada, the Caribbean, Australia, and other international locations. Tyler has been recognized numerous times for growth and innovation, including on Government Technology's GovTech 100 list. More information about Tyler Technologies, an S&P 500 company headquartered in Plano, Texas, can be found at tylertech.com.

CORP-CIO-TL-44433-0426

Empowering people who serve the public®

tyler technologies