

State of the States Forecast: What's in Store for 2024?

January 18, 2024

Doug Robinson, Executive Director

2024 STATE CIO TOP 10 PRIORITIES

Priority Strategies, Management Processes and Solutions

1 CYBERSECURITY AND RISK MANAGEMENT



1 DIGITAL GOVERNMENT / DIGITAL SERVICES



3 ARTIFICIAL INTELLIGENCE / MACHINE LEARNING /
ROBOTIC PROCESS AUTOMATION



4 LEGACY MODERNIZATION



5 WORKFORCE



6 DATA MANAGEMENT / DATA ANALYTICS



7 BROADBAND / WIRELESS CONNECTIVITY



8 IDENTITY AND ACCESS MANAGEMENT



9 CLOUD SERVICES

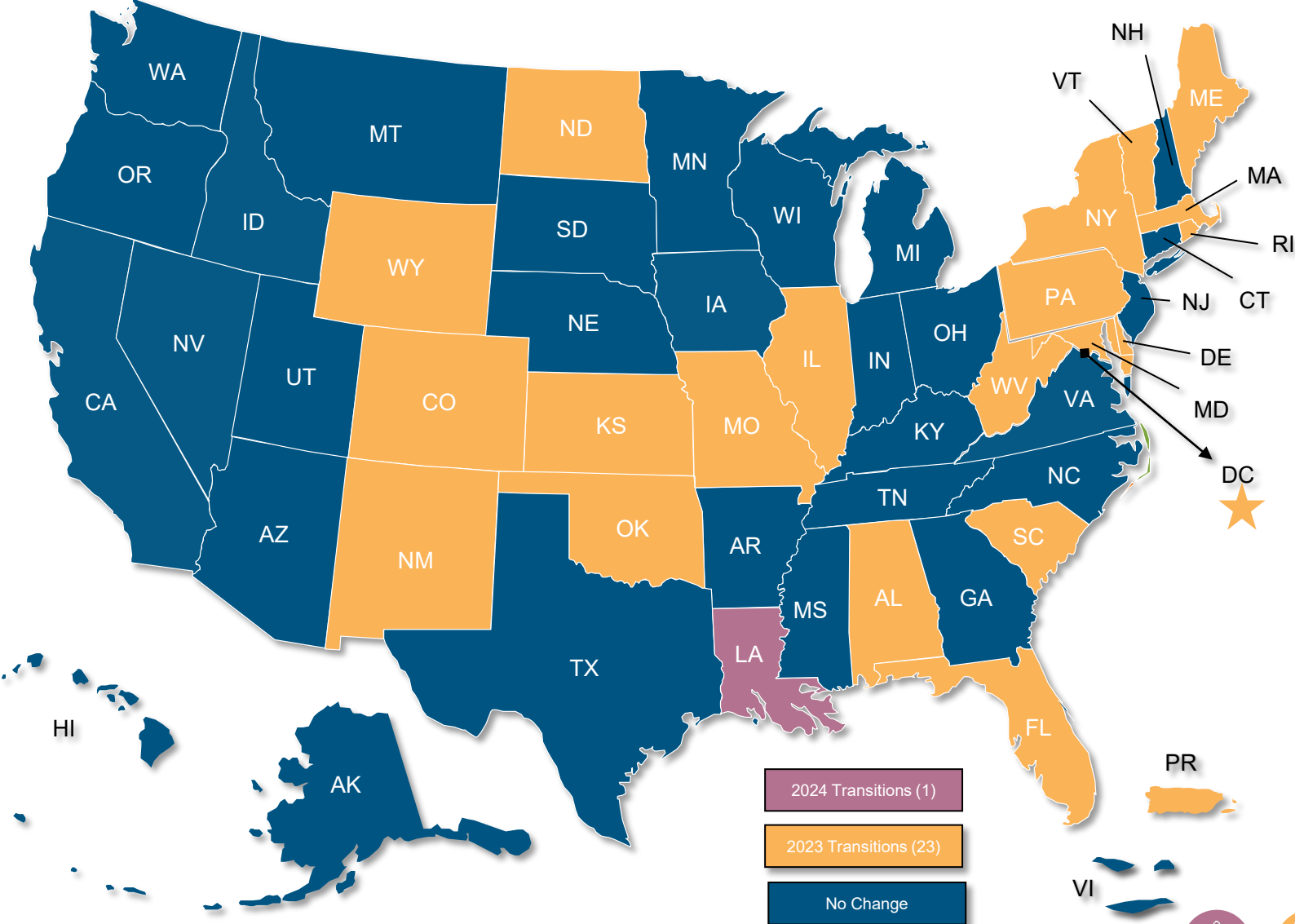


10 CIO AS BROKER / NEW OPERATING MODEL



State CIO Transitions

(January 2024)



Rank the most significant impact to the CIO organization over the next 3 years.

1

Digital services /
citizen experience

2

Cybersecurity

3

Legacy/application
modernization

4

Data governance/
management/
analytics

5

Identity
Management



How will the CIO organization serve customer agencies in the next 3 years? (select all that apply)



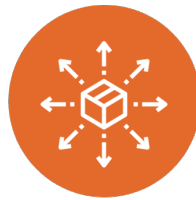
96%

Strategic direction and policy setting



84%

CIO as broker of services



80%

Infrastructure provisioning and operations management



53%

Selective outsourcing



49%

Increase IT employees in the state CIO organization (state employees)



10%

Total outsourcing / managed services



Creating A Citizen-Centric Digital Experience: How Far Have We Come?



October 2023

Calls to Action



**Create an
Enterprise
Vision and
Strategic
Roadmap**



**Engage
Stakeholders**



**Prioritize
Cybersecurity,
Privacy and
Identity
Management**



**Embrace No
Wrong Door**



**Create a
Promotional
Agenda**



**Look Toward
the Future**

Cybersecurity Priorities

Talent crisis: recruitment, retention, reform, compensation

Cybersecurity strategy and risk assessments

More centralized operating model; **zero trust framework**

Adopting **whole-of-state cybersecurity** resilience

Executing Year 2 of \$1B State & Local **cybersecurity grant**

Support and partnerships with **local governments**

Software supply chain risks



Top cybersecurity risks and initiatives

1

Ransomware
attack

2

Agency use
of shadow IT
solutions or
products

3

Human error

4

Compromises
to the software
supply chain

5

Phishing / business
email compromise

State cybersecurity initiatives receiving the most attention are:

1. Endpoint detection
2. Cybersecurity awareness training
3. IAM solution adoption/expansion

How states are recruiting and retaining cybersecurity workers



90%

Offered hybrid or remote work



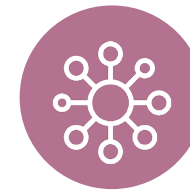
63%

Worked with K-12 and/or higher education to recruit cybersecurity workers



51%

Raised salaries



49%

Collaborated with the private sector, nonprofits, community organizations, federal government or similar groups



45%

Eliminated 4-year degree requirements



What's Trending?

Focus on digital services and modernization: improved **citizen experience**, citizen-centric design, streamlining services, automation, citizen **identity management**

Growing **cloud and SaaS adoption**; reducing IT diversity and complexity - seeking to “rationalize” the technology environment

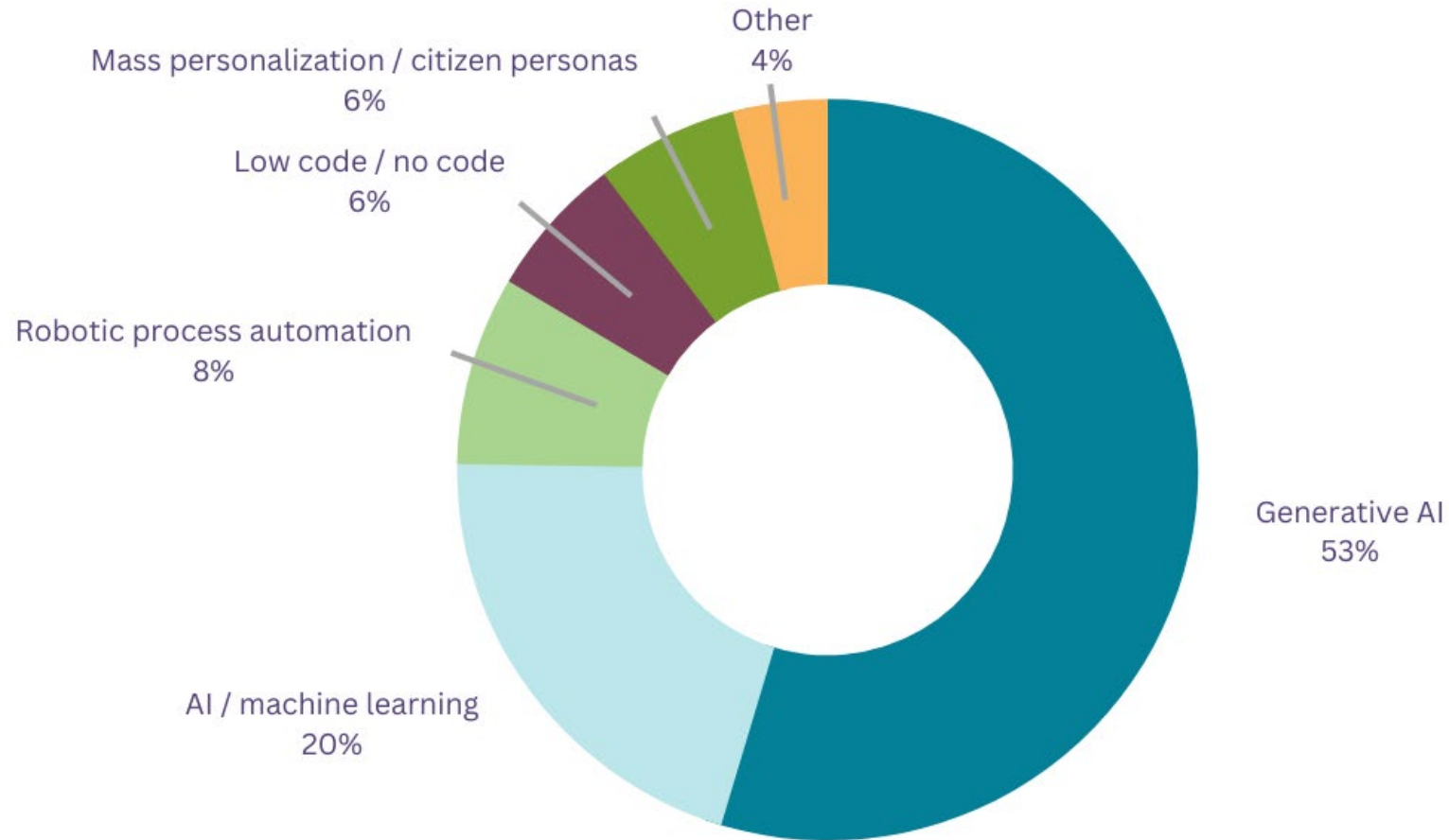
Broader adoption of business **process automation**, chat bots and low code/no code solutions.

Changing IT workforce: **remote/hybrid flexibility**, skills transformation, eliminating 4-year degree requirement

AI and **Generative AI**: governance, legislation (18 states) framework, policy, use cases, data quality, privacy, security, workforce impact

Increase in state tech policy and **legislation**. Focus on data privacy, AI, deepfakes, social media safety, cybersecurity

What emerging IT area will be the most impactful in the next 3-5 years?



Which business process has the most potential benefit from AI in the next 3-5 years?

1

Digital citizen services

2

Cybersecurity operations

3

Fraud prevention and detection

4

Procurement/ acquisition

5

Human resources

6

Licensing and permitting



Your AI Blueprint: 12 Key Considerations as States Develop Their Artificial Intelligence Roadmaps

With the mass availability of generative AI (GenAI) tools and large language models in the last year, states are updating or creating new policies and road maps for artificial intelligence (AI).

The NASCIO State CIO Top Ten Priorities list for 2024 includes artificial intelligence for the first time ever. As AI becomes increasingly integrated into the technology infrastructure of government agencies, an AI roadmap will emerge as an indispensable tool for states in the months and years ahead. An AI roadmap not only facilitates the seamless adoption of AI but also enhances efficiency for an already strained state government workforce.

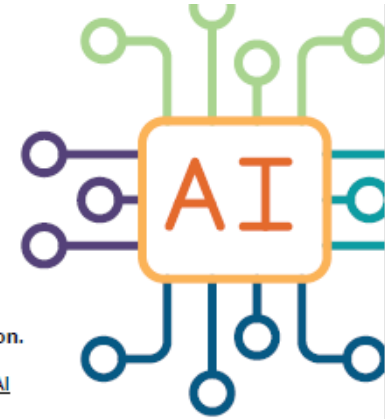
There are several benefits to creating an AI roadmap including improving stakeholder and executive buy-in for AI initiatives, flexibility to adapt as the technology changes, efficient resource allocation and cost savings, risk management and improved service delivery.

Here are a dozen considerations states should include in their AI roadmaps for 2024 and beyond:

- 1 Align AI initiatives to strategic drivers for the organization.** First determine how AI fits into the overall goals of the state IT strategic plan. Don't assume AI will solve every problem or help you reach every goal. In addition, don't go looking for a problem to solve with AI. Identify the business case and overall strategic goals of the organization before deploying an AI tool.
- 2 Establish governance and oversight processes.** Absence of proper AI governance exposes states to potential risks such as data leakage, violations of privacy laws and erosion of citizen trust. To navigate these challenges, it is crucial to adopt established AI governance frameworks such as the [NIST AI Risk Management Framework](#), [OECD Recommendations on Artificial Intelligence](#) and the [European Union AI Act](#).
- 3 Inventory and document existing AI applications.** Discover the extent of AI tools employed by agencies, both knowingly and unknowingly. Some long-standing technology tools have undergone updates to incorporate new AI functionalities.
- 4 Address data quality and sourcing.** Prioritize data governance and classification to ensure the highest quality data available is used. Evaluate data sources, mindful of potential biases.



- 5 Collaborate with stakeholders and industry partners.** Create an advisory board or task force with key stakeholders such as agency heads, the chief information officer, chief privacy officer, chief information security officer, chief artificial intelligence officer, chief information accessibility officer, general counsel and those with expertise in AI ethics. Build industry partnerships to leverage expertise and innovation.
- 6 Assess privacy and cybersecurity risks of AI adoption.** Consider performing privacy and security impact assessments for new AI technologies. Again, the [NIST AI Risk Management Framework](#) can be a useful tool.
- 7 Infrastructure and technology.** Assess the current state of the technology infrastructure and identify areas for improvement. Legacy infrastructure has been a common roadblock for states in the adoption of AI.
- 8 Create acquisition and development guidelines.** Develop best practices and guidelines for acquisition/procurement, development and operation of secure AI systems. Update procurement language as needed to cover AI and generative AI concerns, while also incorporating considerations for accessibility.
- 9 Identify potential use cases.** Research potential use cases of AI by learning from other government entities, organizations and AI leaders. Concentrate on use cases that align most closely to the strategic goals of the state.
- 10 Expand AI workforce expertise and training.** Identify and amplify existing staff expertise, recruit interns and staff, partner with local educational institutions and provide training and educational opportunities for employees. This includes not only technical expertise but also coverage of legal, ethical and policy considerations. Assess positive and negative workforce impacts.
- 11 Create guidelines for responsible use, ethics and transparency.** Ensure that users of AI systems are informed about the risks associated with discrimination and bias. State government should prioritize transparency measures to foster trust among citizens.
- 12 Measure and communicate effectively.** Have clear metrics in place to measure progress and success of AI initiatives. Communicate the outcomes of the metrics with key stakeholders, legislators and other policymakers.



While each state's AI roadmap will be unique to its specific needs, strategic plans and priorities, including these important considerations ensures the establishment of a solid foundation for the seamless integration of AI into state IT initiatives.

Resource Center at NASCIO.org

