

The 2023 State CIO Survey

The Force of
Automation and
the Reality of
Modernization

Table of Contents

Executive Summary	3
Financial Models	4
Cybersecurity	7
Federal Funding	10
Emerging Technology	12
Cloud Services	13
Legacy Modernization	15
Data Management	17
Future Role of the CIO Organization	19
Conclusion	21
List of States Participating in the Survey	22





Executive Summary

Welcome to the 2023 State Chief Information Officer (CIO) Survey, we're glad you're here. We conducted the survey in the summer of 2023 and had 49 state CIO responses to 47 questions on eight topics. As always, our state CIOs provided us with a cache of insightful information. We wanted to know less about plans and aspirations and more about actions and what is happening today. But we still left room for state CIOs to prognosticate on the future of the CIO organization and CIO role. Here's a preview: if there's anyone out there who still doubts that being a good communicator is more important than being a technical expert, please read on.

But before we dig into those questions, we want to share some demographic information. One quarter of state CIO offices have 101 to 299 employees; 22 percent have 1000 or more; and another 22 percent have 300 to 499. The majority of CIOs reported that about 20 percent of their staff are contractors. From this data we can't really say that there have been dramatic shifts overall and that the number of CIO office staff is way up or way down. We can, however, hypothesize that the fluctuations can be attributed to continued consolidation in states and decreased staffing during the pandemic. Finally, on the topic of CIO delivery strategies, we asked how CIO offices will serve customer agencies in the next three years and 49 percent said they would increase information technology (IT) employees in the state (state employees).

We also asked about the CIO organization budget which is \$271 million on average. That of course includes the very large states so the median budget—\$132 million—paints a more accurate picture of the typical CIO organization budget.

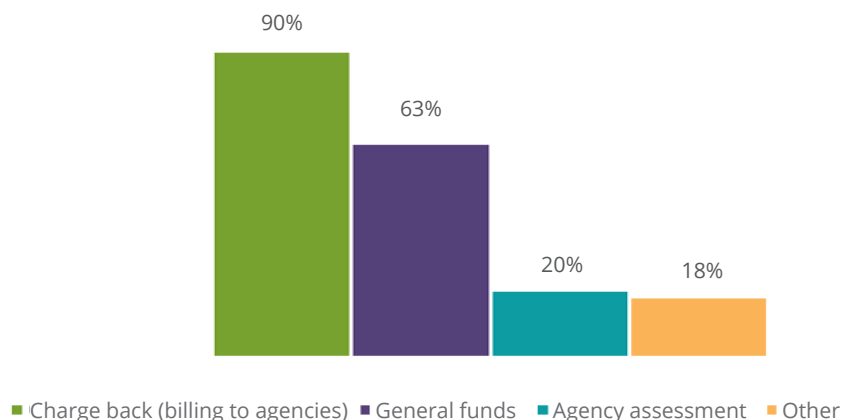
Our survey topics this year include some stalwarts like cybersecurity, emerging technology, cloud services, legacy modernization and data management and also includes some new(ish) topics. We say new "ish" because we might have covered the topics before, but we tried to put a new spin on the questions asked. For example, we asked about CIO financial models because there has been a lot of discussion among state CIOs lately about the optimal model—chargeback, general funds, assessment or hybrid—and we wanted to get a sense of how things *are* and how CIOs think they *should* be. It's no surprise that most states have a substantial chargeback component to their financial model. But many CIOs are working towards obtaining some general funds to be able to tackle modernization, innovation and other projects.

Finally, you'll notice that we didn't include a singular section on workforce but sprinkled workforce questions throughout the survey. Workforce challenges continue to be on the top of mind of every state CIO. States' ability to deliver services currently and in the future is heavily dependent on getting the right people with the right skills and the right number of those folks.

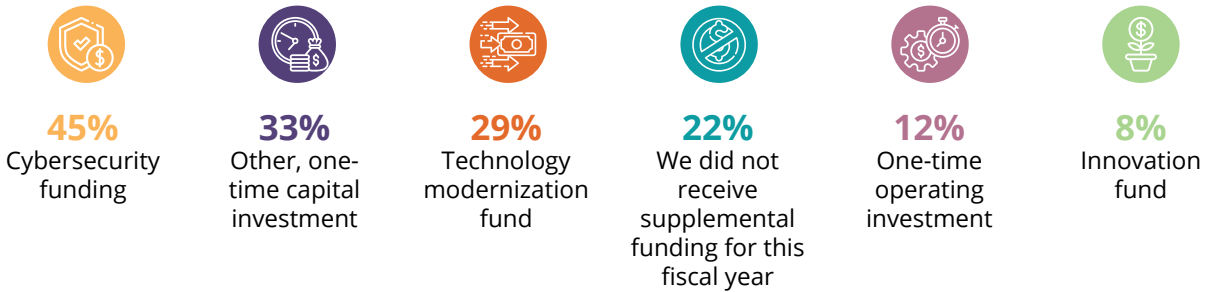
Financial Models

In previous years' surveys, we have asked CIOs about their state's business models, but this year we asked CIOs specifically about their financial models. With only eight states reporting that 100 percent of their revenue comes from a chargeback model (billing agencies), most states are taking a hybrid approach. Ninety percent of states are using chargeback at least partially, while a sizable portion (63 percent) are using general funds as well. A smaller portion (20 percent) chose agency assessment, and several CIOs told us that that other funding sources include federal funding, grants, data sales and appropriated funds.

How is the CIO organization funded?
(Select all that apply)



Has the CIO organization received supplemental funding for the current fiscal year? (Select all that apply)



For those states that use a chargeback billing model, we asked what percentage of total revenue comes from chargeback. While the answers varied from one percent to 100 percent, around three fourths of states (that have chargeback) get over half their funding from this model.

We also wanted to know what percentage of each state's revenue is made up of pass-through federal funds from agencies. For some state CIOs, federal funds are a significant portion of revenue. And, because agencies may be using federal funding to support program delivery, the state must follow federal financial management mandates and appropriately allocate both direct and indirect costs. Almost half of the respondents (46 percent) said federal funds make up less than 20 percent with an additional third of respondents asserting it made up 21 - 40 percent. Only about 17 percent of states said federal funds make up 41 - 80 percent of their revenue.

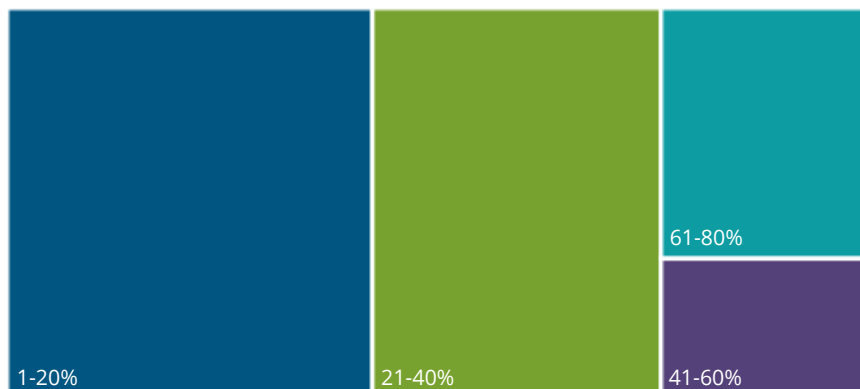
We also wanted to know if the CIO organization received supplemental funding for the current fiscal


year. The most common answer was cybersecurity funding with 45 percent, while other sources included technology modernization funding as well as one-time capital and operating investments.

We also asked state CIOs if the pandemic had an impact on funding for legacy modernization. Three and a half years after the start of the COVID-19 pandemic, we are all aware of its far-reaching impact on governments including how it highlighted the problems associated with aging legacy IT systems. As one CIO said, *"Public expectations have risen around the need for governments to be online."*

Just over half (55 percent) reported that the pandemic did increase funding for modernization, while 39 percent said no, and six percent said they were unsure. Though many states received funding this fiscal year for legacy modernization, it may not continue. As one state CIO explained, *"(Funding increased) during the pandemic when rapid legacy modernization was needed. In our post-pandemic world, COVID-19 is no longer a driver."*

Of your operating revenue, what percentage is made up of pass through federal funds from agencies?





We asked CIOs what the ideal funding model would be for their organization. While responses varied somewhat, the most prevalent response was that an ideal model would be a hybrid of chargeback and general funds. This approach would address the most common complaint from agency customers because CIO overhead charges are embedded in all the rates for services. Many CIOs like the structure and transparency of the chargeback model with the flexibility and innovation that comes from general funds. As one CIO explained, *“Ideally, we would have a hybrid funding model with appropriations for services that are universally needed (ERP, network, licenses, security, disaster recovery) and a chargeback model for optional services.”*

The hybrid model could be useful for innovation and growth as one CIO put it, *“(We should have) chargeback for services, but a general fund allocation for innovation, research and development and similar activities would help IT be much more proactive.”*

“The ideal funding model for our organization would be partial general funds to support core infrastructure needs coupled with a chargeback to agencies for services directly supporting their workforce and business needs.”

Cybersecurity

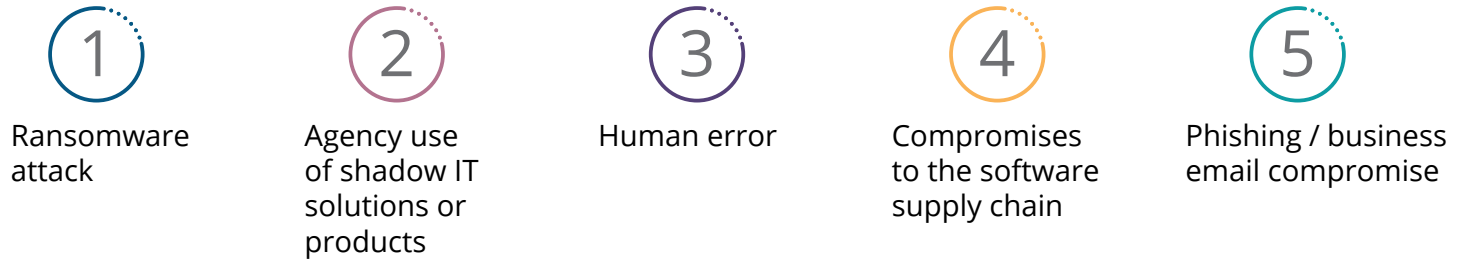
Cybersecurity continues to be THE [top](#) priority of state CIOs for ten years running. For this year's survey we included some longitudinal questions that we ask every few years to check in on the status of cybersecurity programs in states. We also added a few new lines of questioning and tackle foreign-made technology bans and the CIO's role in combatting fraud. But first the

longitudinal questions. When asked to characterize the current status of the cybersecurity program and environment in their states, there aren't any big surprises here. States continue to provide cyber awareness training, adopt the NIST framework and other fundamentals.

Please characterize the current status of the cybersecurity program and environment in your state. (Select all that apply)

	2023	2020	2019
Developed cybersecurity awareness training for workers and contractors	98%	96%	92%
Established trusted partnerships for information sharing and response	92%	89%	82%
Acquired and implemented continuous vulnerability monitoring capabilities	90%	89%	86%
Adopted the NIST Cybersecurity Framework	84%	80%	N/A
Required multi-factor authentication for executive branch agencies	84%	N/A	N/A
Created a culture of information security in your state government	82%	77%	80%
Developed a cybersecurity disruption response plan	80%	66%	61%
Adopted a cybersecurity strategic plan	76%	66%	74%
Required .gov domain for executive branch agencies	71%	N/A	N/A
Documented the effectiveness of your cybersecurity program with metrics and testing	57%	52%	55%
Obtained commercial cybersecurity insurance	53%	55%	47%
Used analytical tools, AI, machine learning and similar approaches to manage cybersecurity program	51%	41%	49%
Adopted a self-insured model for cybersecurity	33%	N/A	N/A
Designed and implemented an antifraud strategy	18%	N/A	N/A

Concerning continuity of government, what is your top cybersecurity risk today?



Interestingly, though, is that 53 percent of states have cybersecurity insurance, just down from 55% when we asked in 2020. With so much discussion lately among state CIOs and state chief information security officers (CISOs), we expected this number could have decreased even more. It is important to note that 33 percent of states indicate they are cyber self-insured.

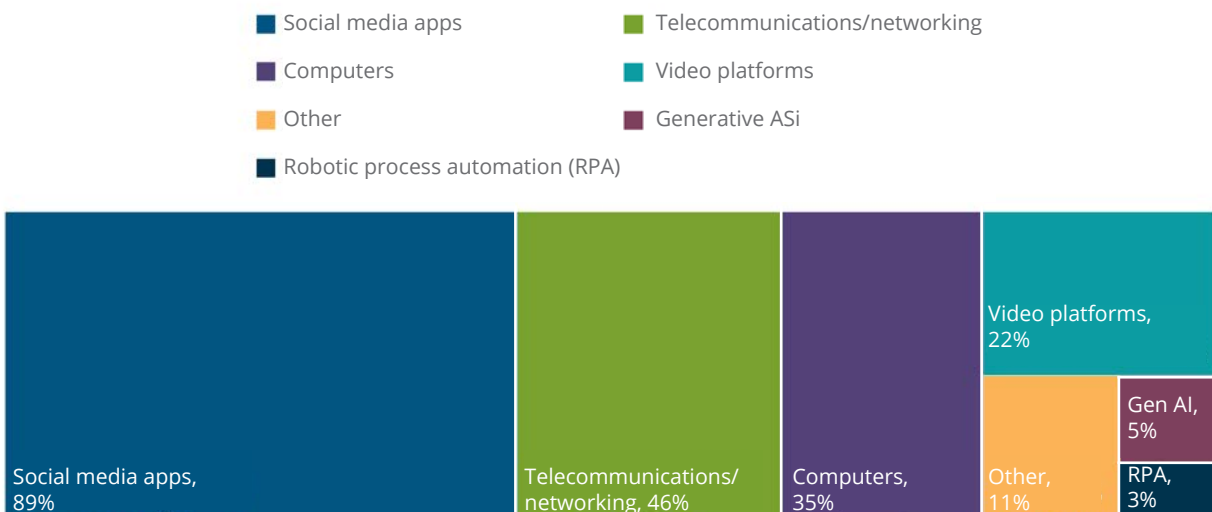
Continuing with fundamentals, ransomware continues to be the top cyber risk as it was when we last asked in 2021. Surprisingly, only 15 percent of CIOs reported that human error is their top cybersecurity risk. We know that human error accounts for a large number of cybersecurity breaches, but we wonder if CIOs are so used to human error that they don't rank it highly?

Finally, on the fundamentals, the state cybersecurity initiatives receiving the most attention are:

- Endpoint detection (80%)
- Cybersecurity awareness training (71%)
- IAM solution adoption/expansion (69%)

We also asked about a few cybersecurity topics that we haven't covered in depth in this survey before. In 2022 and 2023 there have been many headlines about banning foreign technology, social media, application platforms and software due to cybersecurity concerns. Eighty percent of states have banned foreign-made technology, application platforms or software due to cybersecurity concerns and the top two categories banned are social media apps (89 percent) and telecommunications/networking platforms (46 percent). Of those states who have bans in place, most were banned by executive order (54 percent) or enterprise policy (51 percent) and only 32 percent via legislation.

If your state has banned a specific foreign-made technology, application platform or software, which category is banned? (select all that apply)



What actions has your state taken to recruit and retain cybersecurity workers? (Select all that apply)



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

Another topic that has gotten a lot of attention this year, and one that NASCIO has [written](#) on extensively, is cybersecurity workforce. In this year's State CIO Survey, we asked states how they are recruiting and retaining cybersecurity workers. States are offering hybrid/remote work, raising salaries, reworking position descriptions, eliminating four-year degree requirements and focusing on diversity, equity, inclusion and belonging (DEIB), among other things.

A few items of note here. Ninety (90) percent of state CIOs say they are offering *hybrid* OR remote work while, in the 2022 [Deloitte-NASCIO Cybersecurity Study](#), only 25 percent of state CISOs reported that *full* remote work was offered in their states. Anecdotally, we know that more states have gone the hybrid route and that model seems to be commonplace for states offering flexible work. Additionally, 35 percent of state CIOs report they are focusing on DEIB and 29 percent sought out underrepresented communities. This and other recommendations are also included in the joint NASCIO-National Governors Association 2023 publication [Securing States: Modernizing to Attract and Retain Cyber Talent](#). We encourage you to check out that publication for more recommendations on what states can do to retain and recruit cybersecurity workers.

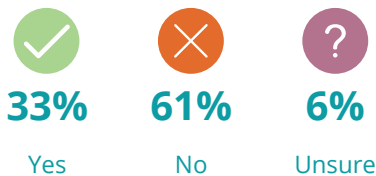
The two, final topics we cover in this section are how states are encouraging local governments to adopt .gov and the CIO's role in combatting fraud. Nearly twenty years after the introduction of the .gov domain, less than ten percent of local governments are registered on the domain. The .gov domain is a [critical](#) component in enhancing public trust in government and includes enhanced security features that are immediately recognized. When asked how they are encouraging adoption of .gov to local governments, the most predominant answer was via awareness, advocacy and education. State CIOs also cited the State and Local Cybersecurity Improvement Act and other state-specific legislation as avenues used.

The last topic we covered in this section is the state CIO's role in combatting fraud. From our earlier question about the status of the cybersecurity program in states, 18 percent of state CIOs say their program includes an anti-fraud strategy. When we asked an open-ended question about whether the state CIO has a role in combatting fraud, we got a mixed bag of responses. The way a CIO answered this question was heavily dependent on the type of organizational model in the state—that is, more centralized states said the CIO absolutely has a role to play in combatting fraud while more federated states generally said this responsibility lies solely with agencies. Still, some CIOs said they are not involved in combatting fraud but that they should or wanted to be.

Federal Funding

In last year's survey, NASCIO noted that states were experiencing a nearly unprecedented level of federal funding. The Coronavirus Aid, Relief and Economic Security Act (CARES), the American Rescue Plan Act (ARPA) and the Infrastructure Investment and Jobs Act (IIJA) all provided states with substantial levels of aid that were intended to address the impact of the COVID-19 pandemic and improve infrastructure. In this year's survey, it's clear that states have worked diligently to direct these funds to their intended uses, and two-thirds of states have obligated all federal funds from previously mentioned legislation.

Does the CIO organization have any unobligated federal pandemic relief (CARES, ARPA, IIJA) funding to support initiatives?



States have used these funds for a variety of purposes, but the most common areas have been directed towards cybersecurity, improving the citizen experience / digital government transition, hardware and software, broadband, legacy modernization and COVID response. For example, one state used CARES funding to purchase hardware and software that

enabled thousands of state employees to transition from in-office to remote work. Several states have been working proactively to deploy broadband funding in underserved areas.

Of those states that have unobligated federal funds, this is generally a result of still-needed legislative approval, working with stakeholders to identify need, waiting on the federal government to release funds, and, especially in the case of the [State and Local Cybersecurity Grant](#) (SLCGP), attaining approval from the relevant agencies on how the state intends to use the money.

The SLCGP is intended to assist states and local communities in addressing cybersecurity vulnerabilities by providing \$1 billion over four years, with a required match and a stipulation that at least 80 percent of funds be directed to local communities. States are allowed to provide services to localities, rather than direct funding, and the majority of states are adopting the shared services approach. Just under ten percent of states are only providing direct funding to local governments with no shared services. The three most common services offered are training, endpoint detection, risk assessments, support for .gov migration and adoption of multi-factor authentication.

Under the State and Local Cybersecurity Improvement Grant, which shared services does your state plan to offer local governments? (Select all that apply)



Cybersecurity training (51%)



Risk assessments (40%)

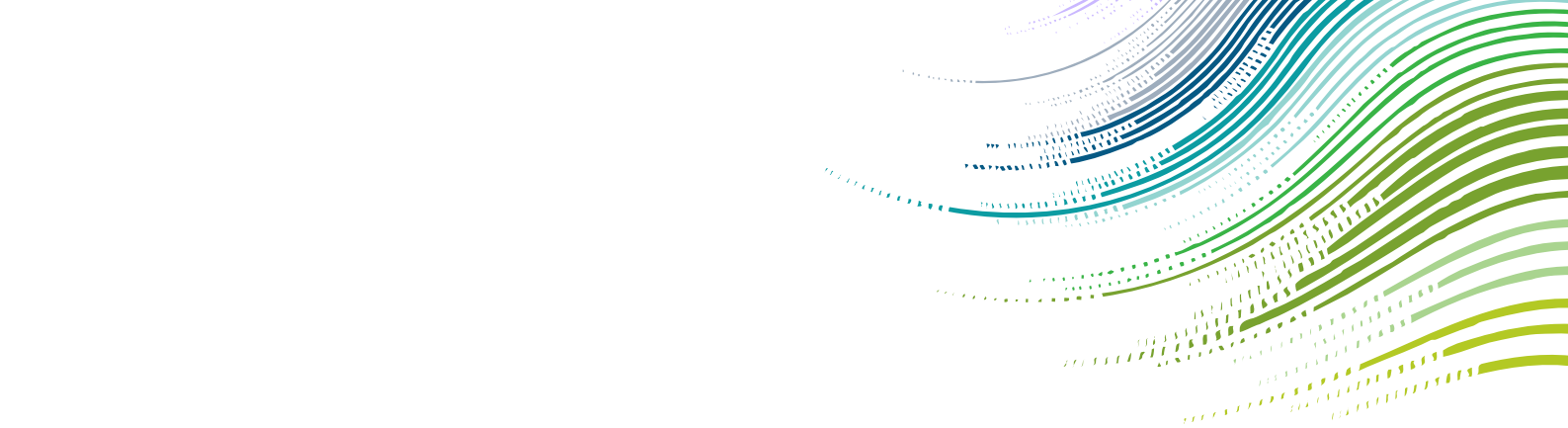


Endpoint detection (40%)

Support for .gov domain adoption	32%
Identity and access management / multi-factor authentication	28%
Security monitoring	28%
Statewide security operations center	26%
Tabletop exercises	26%
Incident response	21%
Governance and oversight	19%
Vulnerability management	19%
Data security/backup/encryption	13%
Network security	13%
Recovery	13%
Managed logging / log alert and auditing services	13%
Ransomware remediation	11%
Web application security	9%
Email security	6%
Configuration management assessments and remediation	6%

While some initial benefits of the SLCGP have already been observed, such as improved coordination between state and local governments on cybersecurity, many respondents raised concerns over how any progress made can be sustained beyond its four-year life cycle. One CIO told us that they were reluctant to launch a new program for local governments, due to concerns it would have to be terminated at the end of four

years. To address these concerns, CIOs recommended increased cost sharing within states, building in sustainability, including local needs in future state contracts and working with legislatures to identify continued funding. A number of respondents also believe that the federal government should do more to help fund any gains made through the program and extend its lifecycle.

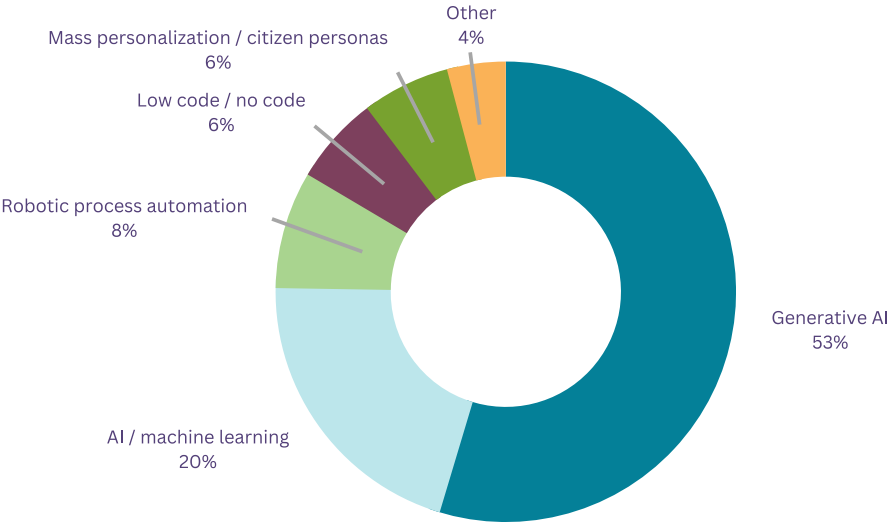


Emerging Technology

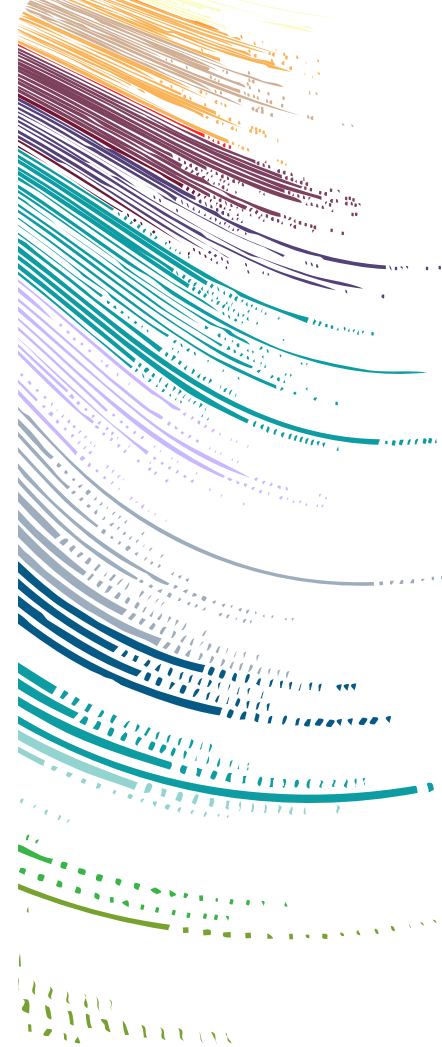
As we have in past years, we asked state CIOs what emerging IT area will be the most impactful in the next three to five years. As new technologies emerge, it's impossible to provide the same answer choices that we did in 2018 or even 2021. Since we last asked this question, generative artificial intelligence (AI) has dominated conversations around emerging technology for state CIOs and was, no surprise, the top answer with 53 percent of respondents choosing it. As one CIO explained, *"Generative AI offers such a significant amplification of speed that it will be evident which organizations are successfully integrating the technology and which are not. But that integration is going to require a fundamental paradigm shift in how we approach work."*

Despite this huge shift in conversation, mainstream AI and machine learning have an important role to play in state government as well, coming in as the second most popular answer with 20 percent of respondents choosing this technology. Though robotic process automation (RPA) only got eight percent, this response most likely reflects the view that RPA is no longer "emerging" but is instead already adopted and in use in many states. *"RPA will be a game changer and awareness of the power of the technology is increasing with the business customers,"* said a respondent to the survey.

Which emerging IT area will be the most impactful in the next three to five years? (select one)



“AI will cause a significant disruption in the next ten years that will fundamentally change the way we work.”



Which business process has the most potential benefit from AI in the next three to five years?

1

Digital citizen services

2

Cybersecurity operations

3

Fraud prevention and detection

4

Procurement/ acquisition

5

Human resources

6

Licensing and permitting

With AI top of mind for state CIOs right now, we wanted to know which business process has the most potential benefit from AI in the next three to five years. We asked CIOs to select their top three choices and they were digital citizen services, cybersecurity operations and fraud prevention and detection. In a 2019 [report](#) from NASCIO, IBM and the Center for Digital Government we asked state CIOs where AI will make the most measurable improvement and impact

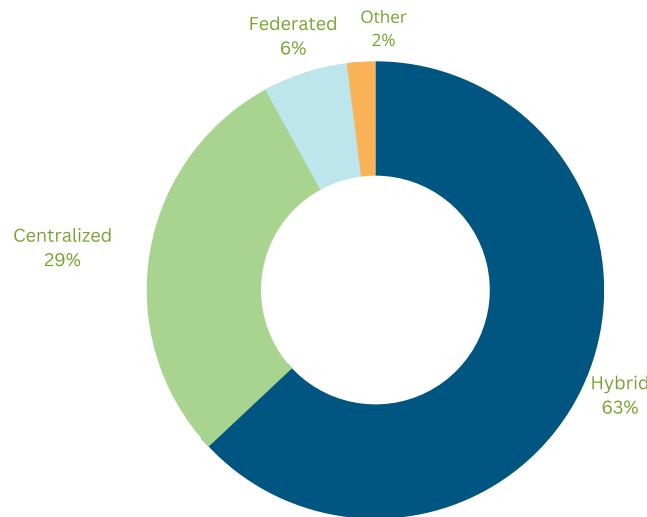
in their state. The top three answers were the same, but in a different order: cybersecurity; fraud, waste and abuse detection; and citizen-facing digital services. No matter how AI is used at the state level, it's clear we are on the cusp of change as articulated by one CIO we spoke with when they said, *“AI will cause a significant disruption in the next ten years that will fundamentally change the way we work.”*

Cloud Services

Cloud services have been explored in many of our previous state CIO surveys via cloud service portfolios, cloud strategies, motivation and justification for moving to cloud services, standards and policy. Cloud services is now an established and critical component of every state government enterprise portfolio—dramatically different from the first year of the State CIO Survey in 2010 when “cloud computing” was considered an “emerging technology.”

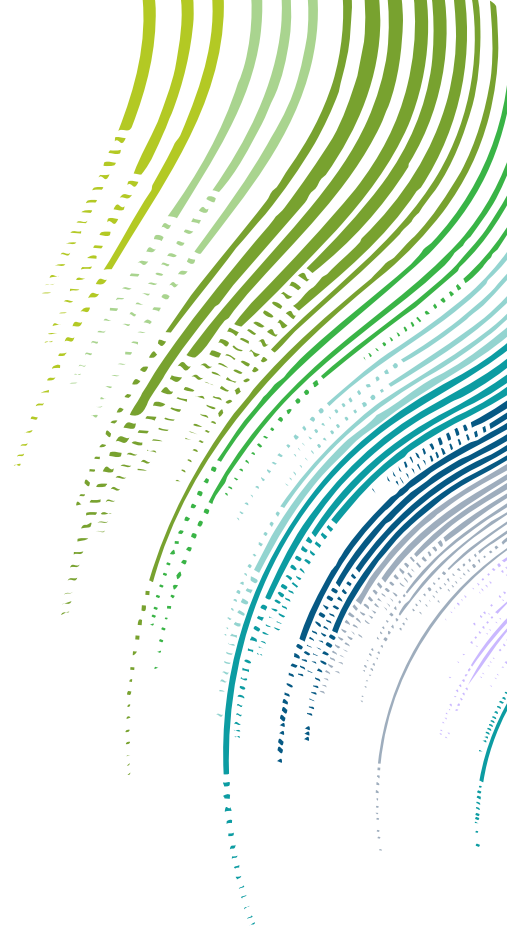
In 2023 we continue our careful consideration of the development of cloud computing by querying state and territorial CIOs some of the same questions for longitudinal understanding of their priorities, their governance and what services are either already migrated to a cloud environment or are on the planning board for future migration. Our first question of state CIOs was regarding their cloud operating model where most states report they are pursuing a hybrid model with a strong minority employing a centralized model.

What is the CIO organization’s cloud operating model?



We next asked state CIOs what categories of services are already migrated to cloud or are in the planning stage. The top of the list of services that states indicate are substantially completed are email/calendar services (94 percent), collaboration platforms (83 percent), service management (47 percent) and project and portfolio management (44 percent). On the other side of the scale, the services that are least completed across the states are data management (0), digital archives (4 percent) and program/business applications (4 percent). It is significant that state government continuity efforts are relying on cloud services to ensure government resilience under challenging circumstances.

What categories of services/functions has your state migrated to the cloud?	Done	Ongoing	Planned	Do Not Know
Email/calendar	94%	6%	0%	0%
Collaboration platforms	83%	17%	0%	0%
Service management	47%	28%	15%	11%
Project and portfolio management	44%	28%	22%	7%
Open data	28%	44%	13%	15%
Mainframe	28%	30%	23%	19%
Identity management	27%	54%	19%	0%
ERP	24%	27%	31%	18%
Human resources / payroll / personnel	24%	38%	27%	11%
Business intelligence / business analytics	22%	63%	8%	6%
Citizen relationship management	22%	47%	24%	7%
Disaster recovery / business continuity	11%	44%	33%	11%
Security	9%	84%	7%	0%
Digital archives	4%	44%	31%	20%
Program/business applications	4%	74%	15%	7%
Data management	0%	77%	16%	7%



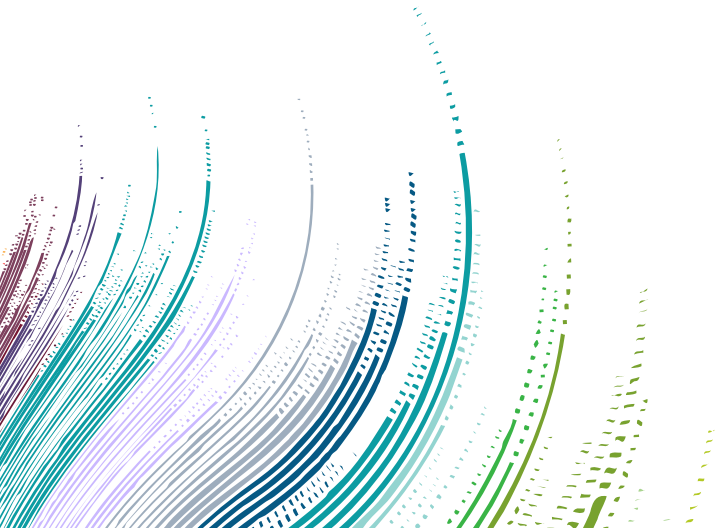
When we asked state CIOs what completed service migrations are off-premise the typical answer was that any migration that was labeled as “done” is indeed off-premise. The top categories of off-premise, completed services were email/calendar, collaboration platforms, service management and mainframe.

The state CIO has been self-described as a strategist, a communicator and a relationship manager in previous state CIO surveys. The role of strategist is particularly important for 2023 when we asked about the state CIO’s authority in making decisions related to cloud services. The majority of state CIOs have full authority for these decisions. The remaining state CIOs share the authority with agencies but play a significant advisory role working with other policy makers and decision makers in a highly collaborative relationship.

No matter what the priority is within state government a persistent challenge is having in place the necessary workforce with the necessary skills. Cloud services have evolved into a highly complex portfolio requiring expertise in acquisition, portfolio management, cost accounting, vendor management, contracting and negotiations. Workforce and workforce skills are a continued challenge to the states’ effective

management of cloud services with nearly 80 percent of respondents stating they do not have the necessary workforce to meet current and future demand.

States are addressing the workforce challenges in different ways and told us that some of the strategies they are adopting are building cloud centers of excellence, hiring additional staff and re-skilling staff in cloud competencies. Managing cloud services continues to increase in complexity involving contracting, procurement, invoicing and managing an emerging and highly complex cloud services portfolio.





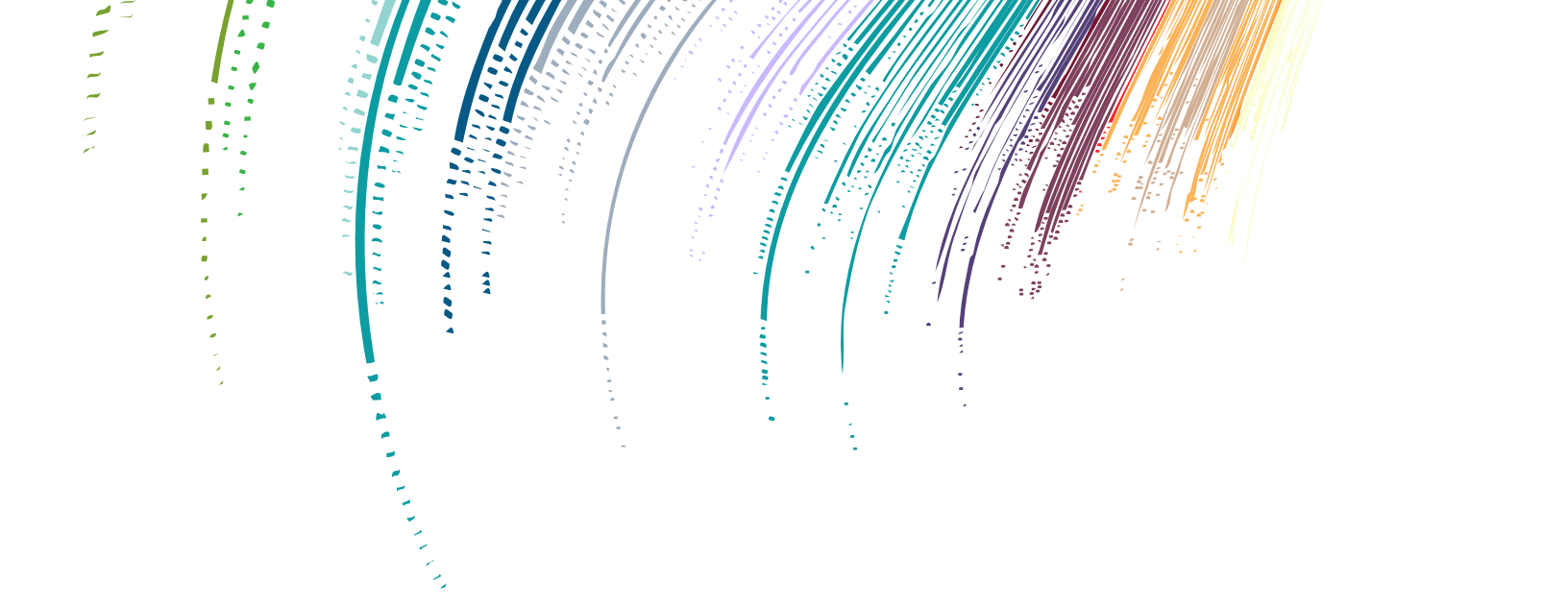
Legacy Modernization

Legacy modernization has remained a priority for state CIOs over many years and has been listed on the [State CIO Top 10](#) almost every year. The burgeoning demand for digital citizen services has pressured state governments to give more attention to legacy modernization as older legacy investments simply cannot meet the capacity and capability demands of the 21st century. Additionally, the advent of the pandemic drove states and territories to ramp up quickly with various systems that were stressed beyond the original design capacity. The response from states in quickly pivoting resources toward remediation and redesign was outstanding. However, states do not want to be in this position ever again. Thus, the motivation to prepare for future crises and also growing expectations for state government responsiveness to citizen needs and demand have kept legacy modernization top of mind for state CIOs.

Earlier in the survey we asked state CIOs if the pandemic was the impetus for increased funding for legacy modernization. Fifty-five percent responded with a definite “yes” while 39 percent said “no” and six percent were unsure. We also asked state CIOs what governance, guidelines and/or policies they had in place to help manage this massive investment and effort. The top responses were: a formal IT review board or steering committee (63%); a cloud strategy for moving applications to the cloud (60%); and an independent third-party to provide validation and verification for large systems efforts (52%). These guidelines and governance are a critical component for managing risk, providing oversight and ensuring legacy modernization efforts stay on track.

What type of governance, guidelines and/or policies does your CIO organization have in place for legacy systems modernization efforts?
(Select all that apply)

Formal IT project review board or steering committee	63%
Cloud strategy for moving applications to the cloud (when feasible)	60%
Independent third-party to provide validation and verification for large systems efforts	52%
Agile project development methodology	50%
Statewide enterprise architecture standards in place for software solutions	50%
The state is moving or has moved to infrastructure-as-a-service or third-party data center hosting; however, applications are still managed by the individual agencies	42%
Established a state technology modernization fund	40%
We prefer a solution integrator	31%
There is no statewide legacy modernization strategy, but agencies are encouraged to leverage the cloud	23%
We let the vendor select a project management methodology	17%
Independent third-party to oversee the technology vendor in a project management organization	15%



In terms of IT modernization, which of the following major lines of business functions have the most technical debt?

1

Human services /
public welfare

2

Health services

3

Corrections

4

Administration/
finance/workforce

5

Labor and
employment

The [NASCIO-VMware report](#) on application modernization provides valuable insights from our research including best practices, valuable strategies to leverage and quick wins to seize early. There is also a recommended timeline for assessment, execution and identifying target opportunities.

Finally in this section, we asked state CIOs about their assessment of the greatest level of technical debt as they look across the agencies and lines of business. For this question, we define technical debt as the cost of maintaining outdated software and systems in lieu of investing in modernization. The most technical debt resides in human resources, health services and corrections. The least technical debt resides in transportation, education and emergency services.

State CIOs offered these comments regarding legacy modernization:

"We are treating legacy modernization as a business and IT strategic partnership that needs to include and align with business process re-engineering, legacy decommissioning strategy, cloud strategy, data strategy and IT Enterprise strategic goals."

"Legacy modernization is a challenge because it's expensive and time consuming. This is where state general funding can help central IT be innovative and have solutions available for agencies to leverage."

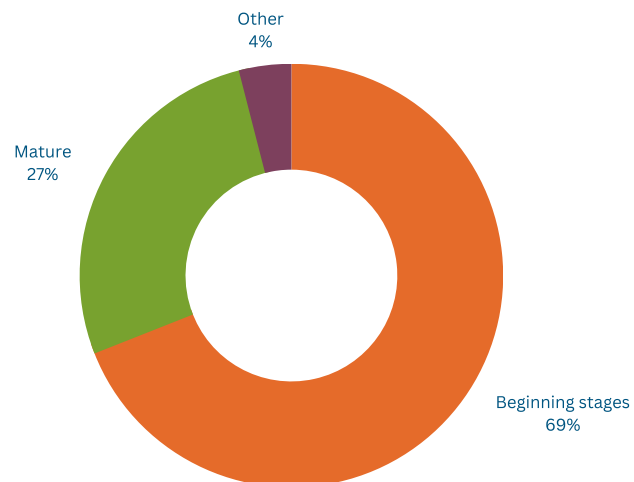
"We are early in our governance efforts. However, we have adopted a start-where-you-are campaign and continue to improve iteratively."

Data Management

Data management remains a primary resource within state government and insight enabling analytics is the means for exploiting this key resource. Data management and analytics have been represented in the state CIO Top Ten priority strategies every year starting in 2016, emphasizing how important this capability is to state government. However, there haven't been great strides in progress in the last several years in this area and there

is room for growth. Case in point, in this year's survey, we asked state CIOs how they would rate the maturity of their enterprise information management discipline. The majority (69 percent) of respondents describe the maturity of their governance structure as being in the beginning stages while 27 percent consider their governance of enterprise information management as mature.

How would you rate the maturity of your governance over enterprise information management?



We also asked state CIOs where they are applying data analytics and the top five responses were: enhanced dashboards and meaningful reports (80 percent); transparency and accountability (71 percent); fraud prevention/detection/response (63 percent); and ease of combining data from multiple sources (57 percent). Only two percent of respondents indicated they are not using data analytics.

We asked state CIOs how they are servicing agency customer needs. It is important to note that only ten percent of respondents stated they are not providing data analytics services to customer agencies.

In which of the following areas does your state currently utilize data analytics? (Select all that apply)

Creating enhanced dashboards and meaningful reports	80%
Transparency and accountability to citizens	71%
Fraud prevention / detection / response	63%
Ease of combining data from multiple sources	57%
Workforce planning and analytics	53%
Surfacing insights from the data, or insight enabling capabilities	45%
Data-driven policy making	43%
More efficient public service delivery	31%
Performance-based budgeting	31%
We do not use data analytics	2%

How does the CIO organization service agency customer data needs? (Select all that apply)

1

Continuing to prioritize providing tools (67%)

2

Procuring needed solutions for customers (63%)

3

Developing data management/ analytics strategies (63%)

4

Defining enterprise policy and architectural standards (57%)

5

Promoting the use of insight enabling analytics (55%)

“While we don’t have a formal data literacy/proficiency program, our leadership and data analysts across the state regularly evangelize the importance of data literacy. This keeps us moving in the right direction in terms of data literacy/proficiency as we look to formalize our programs.”

We queried state CIOs on how they would characterize data management and capabilities within the state CIO organization and what skills they are emphasizing. The capabilities most highlighted were data management, analytics and communication skills. However, challenges remain in delivering data management services, with one CIO telling us, *“We have a small team of folks that are very proficient in these areas, but the demand for them is greater than we have capacity for the moment.”*

The final question we asked in this section is regarding data literacy across state government. Data literacy is intended to increase the level of awareness and ability to leverage data and analytics in decision making. Only 16 percent of state CIOs report that they have a formal data literacy/proficiency program for state employees with 84 percent answering no.

Clearly, we have much ground to gain in this area and it is something that CIOs are pursuing.

Does your state have a formal data literacy/proficiency program for state employees?



16%

Yes



84%

No



Future Role of the CIO Organization

The last section of this year's survey is dedicated to something we love to do—ask CIOs to prognosticate about the future. This year we asked about the future role of the CIO organization and how the state CIO role might change. There were 14 state CIO transitions in 2022 and 21 in 2023 (at the time of publication) which means that two-thirds of current state CIOs were not in their role less than two years ago.

We first asked how customer agencies will be served in the next three years and almost all (96 percent) said it will be driven by strategic direction and policy setting. Next is CIO as broker (84 percent) and then infrastructure provisioning and operations management (80 percent). Only ten percent said they would be completely outsourced.

How will the CIO organization serve customer agencies in the next three 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

“The state CIO office will continue to focus on enterprise architecture and continued/increased collaboration around cyber activities, not only with cabinet level agencies, but with non-cabinet agencies which central IT may not have a deep technical relationship with.”

“The state CIO office will become a visionary role for cross department digital government citizen services.”

We also gave CIOs an opportunity to provide open-ended comments on this question and here are some highlights:

“We will increase state employees in security roles and reduce reliance on contractors for non-specialized roles.”

We also asked CIOs to rank the most significant impact on the CIO organization over the next three years and, overwhelmingly, the top responses were digital services / citizen experience and cybersecurity. There was a large gap between the top two responses and the rest of the field.

Of note here is that consolidation was at the bottom of the list, only receiving votes from two states. However, we know that consolidation is a continuous journey and that states will continue to consolidate.

Finally in this section we asked an open-ended question on how the state CIO role might change in the next three years, and we received a gold mine of responses. Many CIOs mentioned digital strategy and the increased demand for digital services; the transformation of broker of services and innovation; and the demand for CIO-as-broker, procurement and business skills. Some of the best quotes can be viewed on the next page.

1

Digital services /
citizen experience

2

Cybersecurity

3

Legacy/application
modernization

4

Data governance/
management/
analytics

5

Identity
management

“The CIO office is much more collaborative with the agencies and is turning into more of a strategy realization office.”

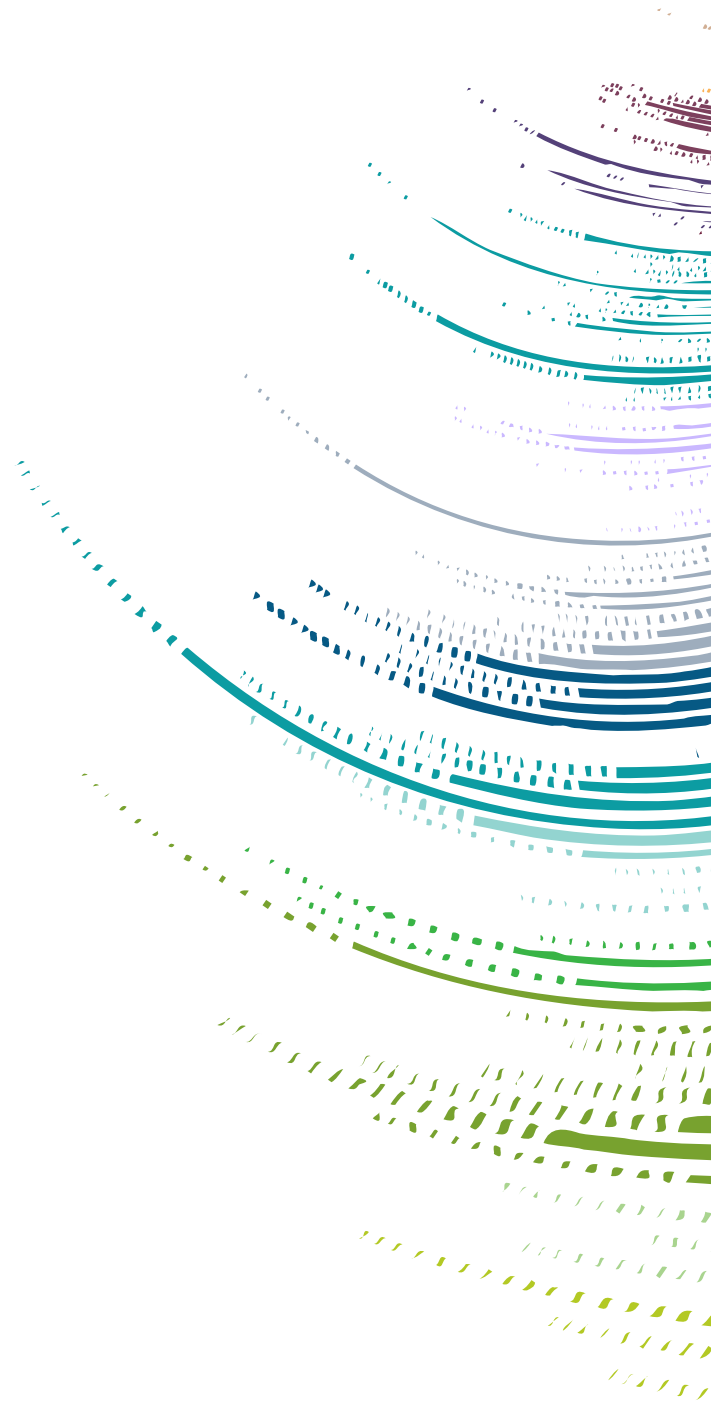
“State CIOs will need to learn to become automation and efficiency experts. The lack of qualified workforce will demand it. Most state organizations have a large percentage of their current workforce already or within a year or two of full retirement age. This will be a critical driver for state CIOs in the next five years.”

“The state CIO’s role evolves at the pace of the industry and, over the next three years, technological advancements and their impact on society will occur at unprecedented levels. AI is the next technology revolution and will change how people work, live and thrive, and will ultimately transform the global economy. State CIOs will chair new technology boards where ethical use and equity policy decisions are determined as each state embraces generative AI, eliminates the digital divide and considers future workforce knowledge, skills and capabilities.”

“The CIO role has gotten a lot more involved in workforce development than in the past and continues to cross over into other domains that were not considered ‘technology’ in the past.”

“The role of the CIO needs to be that of a relationship and transformational leader. It will be important for the CIO to build and maintain business relationships to align, innovate and transform organizational and IT maturity.”

“The CIO is expected to be an evangelist, broker, financial and human resource manager as well as an innovator. The CIO role will continue to evolve where the CIO will be responsible for integrating AI policy and services into state agencies.”





Conclusion

So, what is the most important or pressing issue in this 2023 State CIO Survey? One could argue that they are all important, however, the one area where states must be successful in order to tackle all of these demands is workforce. Workforce challenges, including continuity of leadership, have and continue to have an impact on the state CIO's ability to deliver services both now and in the future. The only way to combat this is for states to embrace reforms and place an increased emphasis on automation. Based on trending adoption, we anticipate further utilization of automation tools and services to streamline business processes; enhance digital citizen experience; and strengthen states' cybersecurity posture. State CIOs in the future will continue to face significant technical debt and challenges with modernizing the state's technology environment. Perhaps the most important characteristic of a modern state CIO will be the ability to lead through change.

List of States Participating in the Survey

State of Alabama

Daniel Urquhart
Secretary of Information
Technology

State of Arizona

J.R. Sloan
State Chief Information Officer

State of Arkansas

Jonathan Askins
Director of Transformation and
Shared Services' Division of
Information Systems & Chief
Technology Officer

State of California

Liana Bailey-Crimmins
Chief Information Officer and
Director

State of Colorado

Anthony Neal-Graves
Chief Information Officer

State of Connecticut

Mark Raymond
Chief Information Officer

State of Delaware

Gregory Lane
Chief Technology Officer

District of Columbia

Michael Rupert
Interim Chief Technology
Officer

State of Florida

James Grant
Former Chief Information
Officer

State of Georgia

Shawnzia Thomas
State Chief Information Officer

State of Hawai'i

Doug Murdock
Chief Information Officer

State of Idaho

Alberto Gonzalez
Chief Information Officer

State of Illinois

Sanjay Gupta
Secretary and State CIO

State of Indiana

Tracy Barnes
Chief Information Officer

State of Iowa

Matt Behrens
Chief Information Officer

State of Kansas

Jeff Maxon
Interim Chief Information
Technology Officer

Commonwealth of Kentucky

Ruth Day
Chief Information Officer

State of Louisiana

Richard Howze
State Chief Information Officer

State of Maine

Nicholas Marquis
Acting Chief Information Officer

State of Maryland

Katie Savage
Secretary of Information
Technology

**Commonwealth of
Massachusetts**

Jason Snyder
Secretary and Chief Information
Officer

State of Michigan

Laura Clark
Chief Information Officer

State of Minnesota

Tarek Tomes
Commissioner and Chief
Information Officer

State of Mississippi

David Johnson
Chief Information Officer

State of Missouri

John Laurent
Acting Chief Information Officer

State of Montana

Kevin Gilbertson
Chief Information Officer

State of Nebraska

Ed Toner
Chief Information Officer

State of Nevada

Timothy Galluzi
Chief Information Officer

State of New Hampshire

Denis Goulet
Commissioner / Chief
Information Officer

State of New Jersey

Christopher Rein
Chief Technology Officer

State of New York

Jennifer Lorenz
Acting State Chief Information
Officer

State of North Carolina

James Weaver
Secretary and Chief Information
Officer

State of North Dakota

Kuldip Mohanty
Chief Information Officer

State of Ohio

Katrina Flory
Chief Information Officer and
Assistant Director

State of Oklahoma

Joe McIntosh
Chief Information Officer

State of Oregon

Terrence Woods
Chief Information Officer

**Commonwealth of
Pennsylvania**

Patti Chapman
Acting Chief Information Officer
(former)

State of Rhode Island

Brian Tardiff
Chief Information Officer

State of South Dakota

Jeff Clines
Chief Information Officer

State of Tennessee

Stephanie Dedmon
Chief Information Officer

State of Texas

Amanda Crawford
Executive Director and Chief
Information Officer

State of Utah

Alan Fuller
Chief Information Officer

State of Vermont

Denise Reilly-Hughes
Chief Information Officer

U.S. Virgin Islands

Rupert Ross
Director and Chief Information
Officer

Commonwealth of Virginia

Robert Osmond
State Chief Information Officer

State of Washington

William Kehoe
Director and Chief Information
Officer

State of West Virginia

Josh Spence
Former Chief Information
Officer

State of Wisconsin

Trina Zanow
Chief Information Officer

State of Wyoming

Tim Sheehan
Acting Chief Information Officer



About the National Association of State Chief Information Officers

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs.

Primary Authors

Doug Robinson, Executive Director

Meredith Ward, Deputy Executive Director

Authors and Contributors:

*Amy Glasscock, CIPM, Program Director,
Innovation and Emerging Issues*

*Emily Lane, Director of Experience and
Engagement*

*Eric Sweden, MSIH, MBA, CGCIO, Program Director,
Enterprise Architecture and Governance*

Alex Whitaker, Director of Government Affairs