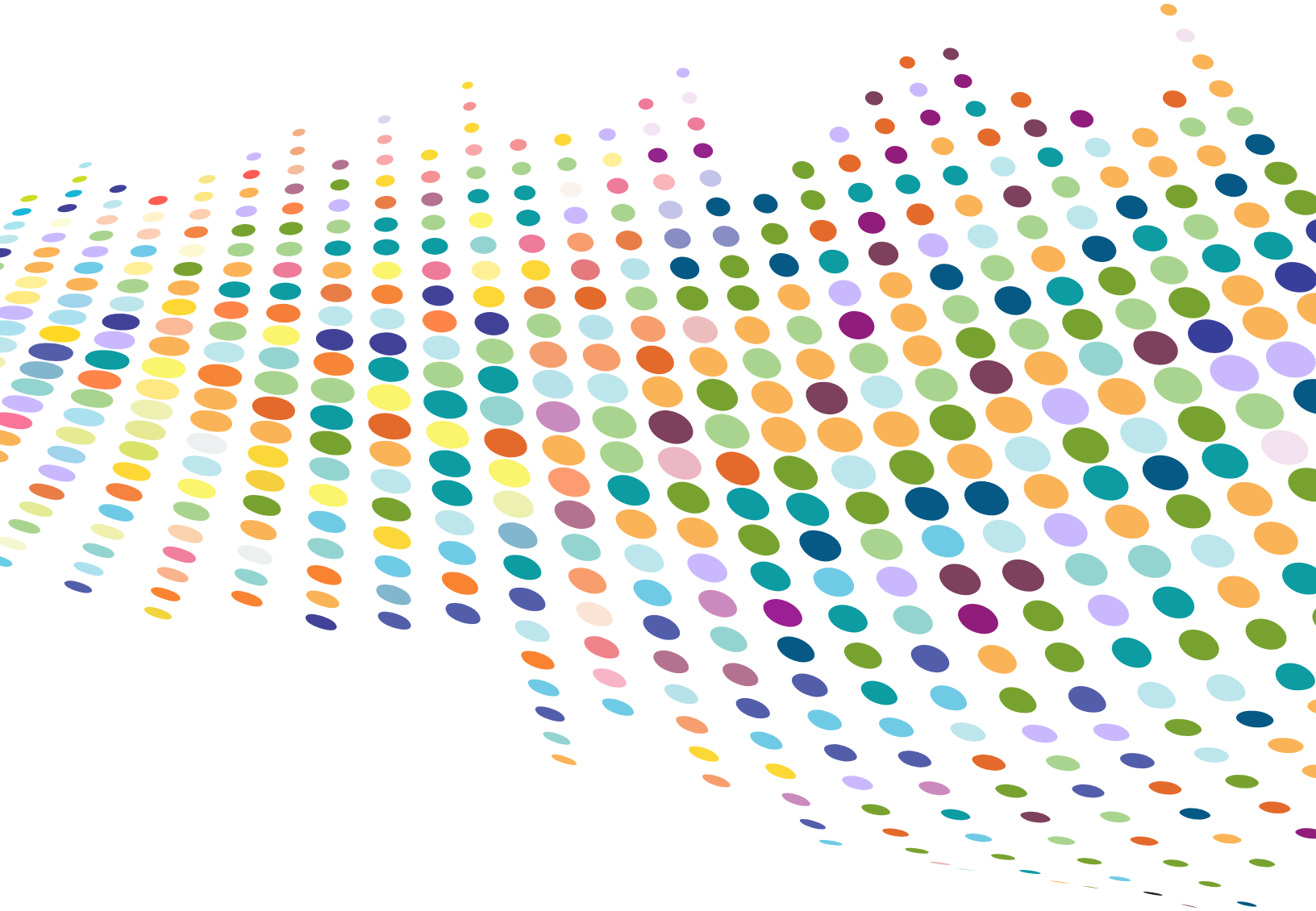
Privacy Persevering:

How State Chief Privacy Officers Are Advancing Governance With Limited Resources

The 2026 State Chief Privacy Officer Survey

April 2026



NASCIO®
Representing Chief Information Officers of the States

Evolution of the State CPO Role

In this fourth NASCIO state chief privacy officer (CPO) survey, we see the role grow in leaps and bounds. In **previous years**, we saw the number of state CPOs increasing steadily due to an avalanche of data created by digital government, public state data breaches and a demand from citizens who are increasingly concerned about their private information. This momentum has continued and today, the number of states with a CPO (or someone who handles privacy at an enterprise level) is now 31. In addition, the federal government, despite several attempts, has not passed a comprehensive privacy law, which has motivated **21 states at the time of this publication** to pass their own legislation. Other states are sure to follow suit in the coming year.

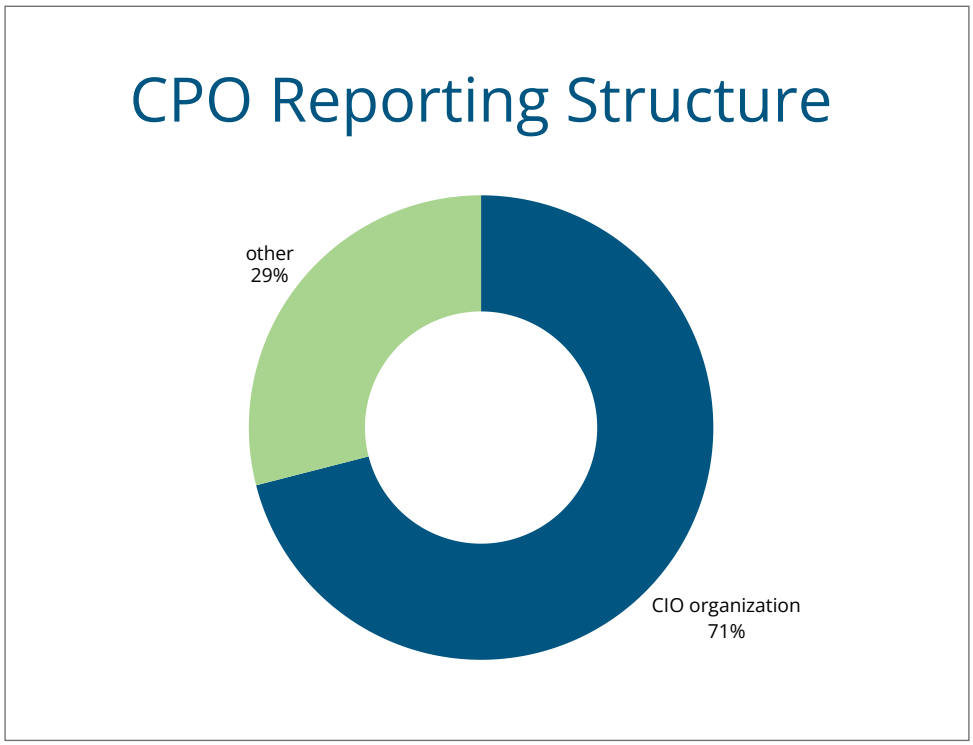
Of the 31 states with a CPO position, 28 of those positions were filled at the time of the survey, all of whom participated. Forty-three (43) percent of CPOs are the first to hold the role (as it's currently defined) in their state. Privacy governance is becoming more established in the states at the same time the explosion of artificial intelligence (AI) in use in states has played a significant role in privacy and in the daily work of state CPOs. State CPOs are seeing privacy buoyed by the elevation of artificial intelligence (AI)—while they simultaneously fear it could be overshadowed by it as a priority.

Number of State CPOs by Year

Year	Number of CPOs
2005	1
2010	3
2015	7
2020	17
2025	31

The CPO Role Today

Not all state privacy leaders have “chief privacy officer” in their title, but 75 percent of them do (or similar such as privacy program manager). Eighteen (18) percent have a general counsel role and handle privacy as part of it. There is even some overlap with five state CPOs saying they have both “privacy” and “counsel/legal” in their titles.

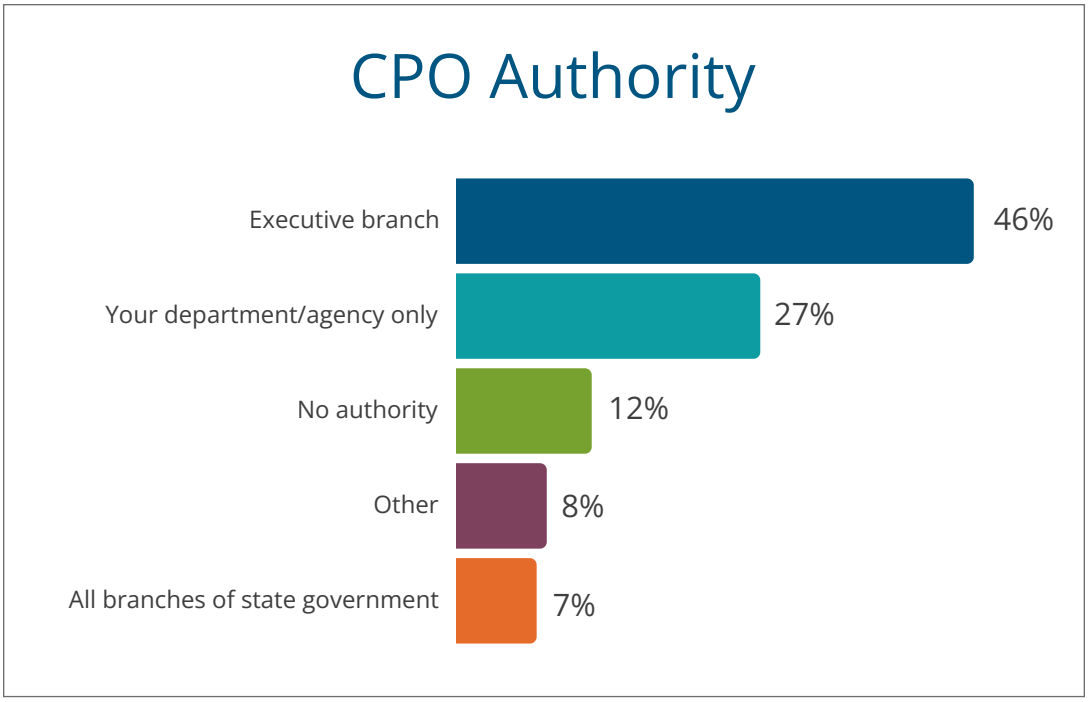


Today the state CPO is most likely to be found in the CIO organization (71 percent). They report to the state chief information officer (CIO) (36 percent), deputy CIO, state chief information security officer (CISO) or legal counsel within the CIO organization. The other 29 percent report to another entity outside of the CIO organization such as the chief data officer, deputy chief legal counsel or an official in the governor’s office. As we have said in prior years, it is much less common in the private sector for a CPO to report to the CIO or CISO—most commonly privacy resides in legal or under the general counsel in the private sector.

Reasons for the difference between states and private companies could include the fact that in state government, the technology agency is often seen as an agency that oversees the enterprise for compliance purposes, is heavily involved in handling data, integrally involved in risk management and is taking the lead on AI which privacy officers are increasingly involved in. NASCIO has also been championing the role for over a decade and that could have some influence on state CIOs directly hiring CPOs under the technology umbrella.

This year, 43 percent of CPOs report that they have privacy staff that report to them (up from 35 percent in 2024). The average number of privacy staff ranged from two to eight with a median of three. The most common roles were deputy chief privacy officer and privacy analyst. Lack of qualified staff was a top challenge for CPOs in 2024, so it’s encouraging to see that strides have been made.

We asked CPOs about their scope of authority. Forty-six (46) percent have authority over the executive branch agencies, 27 percent over their agency only and 12 percent say they have no authority. Some commented that while they only have authority over their agency, they can provide training and guidance to other executive branch agencies.



We asked state CPOs if they consider privacy in their state to be centralized, decentralized or hybrid. Sixty-four (64) percent said privacy is a hybrid of these in their state and 36 percent chose decentralized. Nobody chose fully centralized.

Who State CPOs Are (and Why it Matters)

Given the common overlap between privacy and legal, it's probably no surprise that 71 percent of state CPOs hold a Juris Doctor degree (JD) and are currently or previously involved in legal and compliance issues for the state. This number is similar to what we've seen in past years.

We asked CPOs about the professional experience that led to their current role in privacy for the state. The following themes emerged:

- **Legal and compliance foundations.** Most CPOs come from legal, attorney general or compliance roles, with experience in privacy law, public records, contracting and regulatory enforcement.
- **Agency-level privacy and data governance experience.** Many served as privacy officers, privacy counsel or data-governance leads within agencies before moving into statewide roles.
- **Handling sensitive data and data-sharing.** Common backgrounds include managing public records requests, negotiating data-sharing agreements and overseeing highly sensitive data (e.g., health, workforce, education and justice).

- **Technology, cybersecurity and operational experience.** A substantial number bring expertise in technology policy, cybersecurity, data science, enterprise technology and translating privacy requirements into operational practice.
- **Public-sector leadership and building trust.** Paths frequently include cross-agency leadership, civil rights or consumer protection work and direct involvement in building statewide privacy policy, governance and law.

Given state CPOs' range of expertise from legal and compliance, data governance, security, technology and government, it's no surprise that they are regularly pulled into both AI governance and enterprise risk discussions.

We also wanted to know if state CPOs are obtaining certifications in privacy and 54 percent have at least one. The most popular certification is the Certified Information Privacy Professional (CIPP) certification from IAPP with 13 CPOs holding it. Second was the Certified Information Privacy Manager (CIPM) certification from IAPP (six CPOs). Four state CPOs have earned the new IAPP Artificial Intelligence Governance Professionals (AIGP) certification. One is an IAPP Fellow of Information Privacy. A few reported training for the certifications but have yet to take the exam.

Privacy Program Maturity

Over the last two years, states have been hard at work establishing and maturing their privacy programs. This year, 29 percent report having an established privacy program (up from 24 percent in 2024), 54 percent report that the program is in the process of being developed (up from 41 percent in 2024) and only 18 percent report that they have no privacy program (down from 35 percent in 2024.)

Status of State Privacy Programs

2026	
Established	29%
Not established	18%
In process	54%

2024	
Established	24%
Not established	35%
In process	41%

In 2024 the number one thing CPOs said they needed to do their job effectively was a privacy governance structure—and it's incredible to see how much privacy governance has evolved in just two years. At that time only four states reported using a framework for privacy—three of them used NIST and one used "privacy by design" principles. This year 22 states (79 percent) reported using the NIST privacy framework and eight (29 percent) follow "privacy by design"

principles. Four states reported that their framework is based on the **Fair Information Practice Principles** and two reported state-specific frameworks. This is the single largest indicator of maturity in state privacy programs over the last two years!

Digging a little deeper, we asked what steps state CPOs have taken to implement or operationalize the framework for their business units. The top five were the following:

1. Developing privacy rules, policies, statements and guidance **(82%)**
2. Establishing training and/or certifying points of contact in each agency **(61%)**
3. Implementing data sharing agreements **(54%)**
4. Conducting state-wide privacy training **(50%)**
5. Conducting privacy impact assessments **(46%)**

Privacy training continues to increase in states. Twenty-nine (29) percent are specifically training agency privacy leads as part of their program. As for training the rest of the state government workforce, 32 percent report that they offer mandatory privacy training with another 14 percent offering optional privacy training. Five state CPOs mentioned that privacy training is included as part of the mandatory state cybersecurity training as this seems to be an easier way to get privacy training out to state employees. One CPO told us,

> ***Last year was the first year we had mandatory training, and we added it into the long-standing cybersecurity training.***

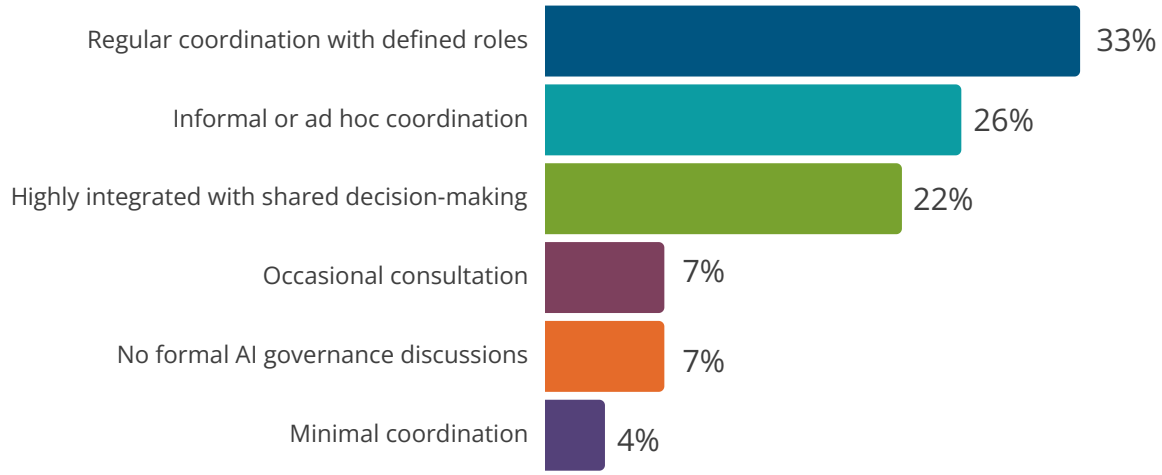
Privacy and AI Governance

We asked if CPOs were involved in setting policies related to artificial intelligence and 90 percent said yes (compared with 77 percent in 2024). This year, we wanted to know more about how CPOs are involved in AI-related activities. The top five answers were the following:

1. AI policy development **(90%)**
2. AI risk assessments **(68%)**
3. AI procurement review **(61%)**
4. Vendor AI due diligence **(43%)**
5. AI incident response **(36%)**

We also wanted to know how CPOs would characterize collaboration between the CPO, CIO and CISO on AI-related privacy risks. Only 22 percent said the collaboration is highly integrated with shared decision making, but a third (33 percent) say they have regular coordination with defined roles. Around a quarter (26 percent) said collaboration is informal or ad hoc. Eighteen (18) percent said collaboration was either occasional, minimal or there were no formal governance discussions.

Collaboration Between CPO, CIO and CISO on AI-Related Tasks



Most CPOs (89 percent) said the most impactful data points when communicating AI-related privacy risks to CIOs, CISOs or executive leadership is the "type and sensitivity of the data used or exposed." At least one CPO argued that the most impactful data point might be different for a CIO, a CISO or an executive in leadership. The top three most impactful data points overall were the following:

1. Type and sensitivity of the data used or exposed **(89%)**
2. Likelihood of harm to individuals **(56%)**
3. Reputational or public trust impact **(51%)**

When it comes to assessing privacy risks related to AI, we wanted to know what kind of approach is used most. About a third of respondents said that they either have no consistent or formal risk scoring approach, or an assessment is currently in development. Of those that do have an approach, the most popular answer was "integrated into an enterprise risk management framework" at 21 percent. A handful of states said that their approach is aligned with cybersecurity risk scoring or based on privacy impact assessments.

Approaches Used to Assess or Score AI Privacy Risks

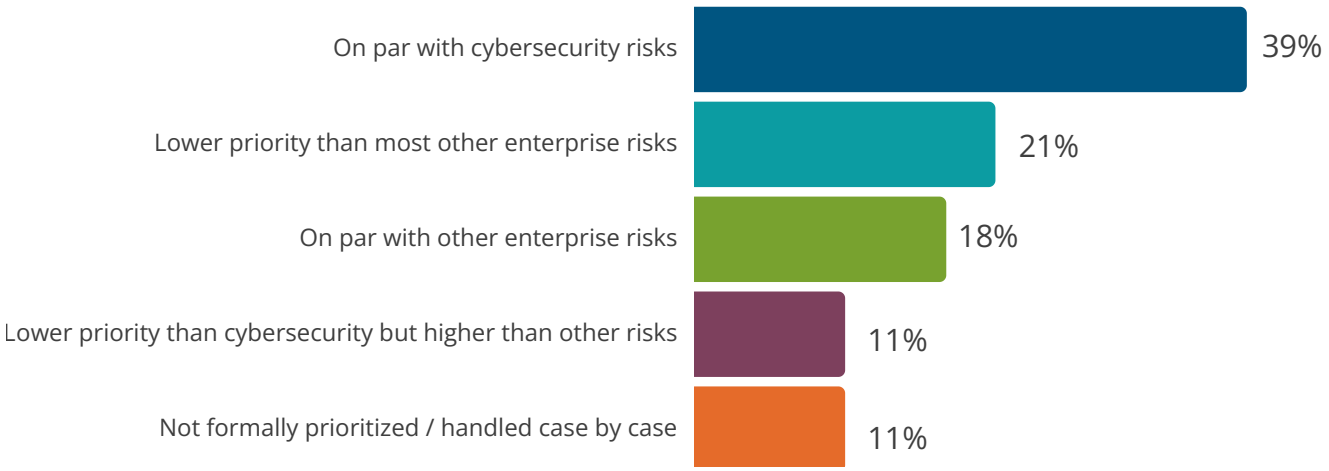
Given the complexity of governing AI today, it seems most states that have a CPO are finding value in including them at the table with CIOs and CISOs. As one CPO said,

> ***Each of our roles adds value from our subject matter expertise, but the real value is created when we break down operational and process siloes to collaborate together about business outcomes, risks vs tradeoffs, priorities, operating models, frameworks, governance and culture change.***

Privacy as Enterprise Risk

Over the last decade, privacy as a priority has been emerging, while cybersecurity has been top of mind for state CIOs (topping the CIO Top 10 Priorities list for 13 years until AI took the top spot this year). We asked state CPOs how privacy is prioritized relative to other enterprise risks in their state (e.g., cybersecurity, operational, financial, legal, reputational and third-party vendors) and it seems that privacy is increasing in priority. Thirty-nine (39) percent say that privacy-related risks are prioritized on par with cybersecurity risks, 11 percent said they are a lower priority than cybersecurity, but higher than other risks, and 18 percent said they are on par with other enterprise risks. Unfortunately, 21 percent report that privacy is a lower priority than most other enterprise risks and eleven percent said privacy is not formally prioritized or it's handled on a case-by-case basis.

Privacy-Related Risks Prioritized Compared to Other Enterprise Risks



Automation and Procurement Processes

Given the privacy implications of purchasing and using technology, state CPOs are often included in the procurement approval process. Sixty-eight (68) percent say they are involved while 32 percent say they aren't. Some did say that their agency is involved, or they are occasionally asked to review the contracts, sometimes as an afterthought. As one CPO said,

> ***I don't review all contracts and I'm usually the last person asked to review (so I am given minimal time and usually pressed for a quick review) as the contract has already been awarded and all other language negotiated.***

State CPOs use a broad range of tools to standardize and automate privacy tasks and processes. The most common tools are training and awareness platforms (69 percent), reporting, metrics and executive dashboards (39 percent), intake, forms and low-code workflow tools (35 percent).

Tools Used to Standardize and Automate Privacy Tasks and Processes

Training and awareness platforms	69%
Reporting, metrics and executive dashboards	39%
Intake, forms and low-code workflow tools	35%
Other	31%
Privacy management platforms for PIAs	23%
Data mapping and inventory tools	19%
Incident and breach management tools	19%
AI and automated decision-making risk tools	4%

Budget, Enforcement and Limits of Authority

A defined budget for privacy continues to be a real challenge for state CPOs. Only six states reported having a defined privacy budget (up from three states in 2024) with four of those coming from appropriations, two from agency allocations and one from grants. Of those six states, over the last two years, three reported their budgets increased, one remained the same and one decreased due to across-the-board budget cuts.

While we learned earlier that 46 percent of state CPOs have authority over the executive branch agencies, we wanted to know how many of them have the authority to enforce compliance with enterprise policies in the executive branch. Thirty-six (36) percent said that they do, 29 percent say privacy policies are not enforced and 11 percent say privacy policies are enforced by another entity. Seven respondents chose the "other" option for reasons such as:

- Their agency has no privacy policies to enforce
- Privacy policies are enforced at the agency level
- Their agency provides recommendations only
- They only have authority when tied to the procurement approval process

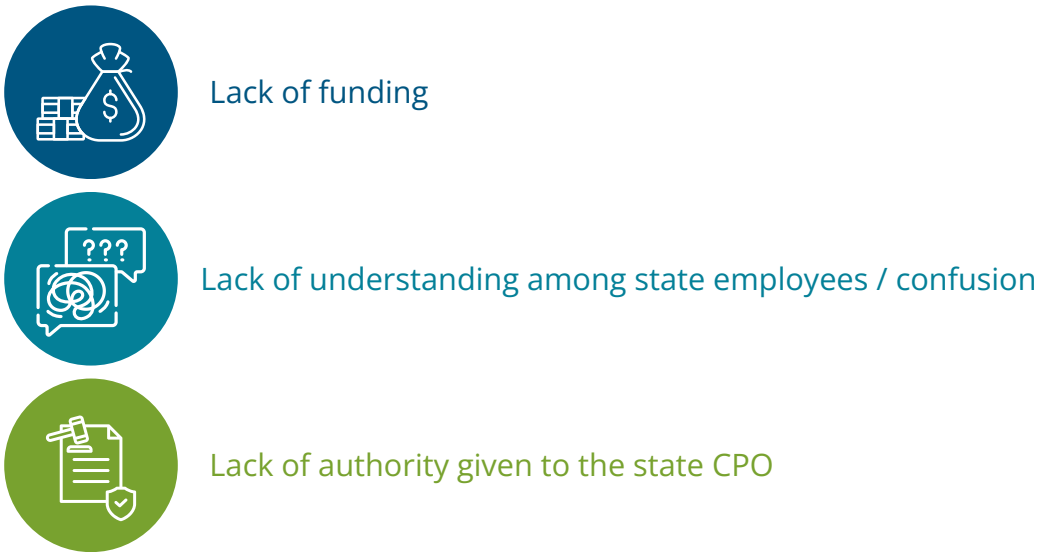
We can see here the tough spot that privacy is in today. Almost half of state CPOs are given authority over the executive branch, over a third of them are tasked with enforcing privacy policies in the executive branch, but only 21 percent of them have a defined privacy budget. It's understandable why they list lack of budget as their top challenge and funding as their top need (see next section).

What CPOs Need Most

As in previous years, we asked state CPOs what their top three challenges are, and we see similar themes as in the past. Lack of funding for privacy initiatives comes in at the top spot with 64 percent. The second most common answer was the lack of understanding among state employees and confusion about what privacy is (54 percent). The third most common answer was about the lack of authority given to the state chief privacy officer (50 percent, which is similar to the number of CPOs that don't have authority over the executive branch).

Most state CPOs are not struggling with knowing what to do—they are struggling with having the authority and capacity to do it consistently.

Top 3 Challenges for CPOs



We also asked about the top five items/resources that they need to do their job effectively. While the answers were split, it's no surprise that the top answer was adequate funding. Again, with only six states reporting a dedicated privacy budget, most states are doing the best they can with very little funding.

Coming in at number two for the first time was "support of the state CIO." This is understandable given the high number of CPOs that are in the CIO organization. In the same vein, the third most common answer was "support of the governor or other senior state management leaders." As one state CPO commented,

> ***Support of the state CIO provides a necessary foundation for success as this individual has been able to garnish support of the governor, state agencies and other senior state leaders.***

Top 5 Things CPOs Need to Do Their Job Effectively

1. Adequate funding
2. Support of the state CIO
3. Support of the governor or other senior state leaders
4. Adequate staffing
5. Enforcement ability

A need for privacy governance was the top challenge in 2024, but states have come a long way. Only 29 percent said they need an effective privacy governance structure this year.

Advice for States New to Privacy

Some of the state CPOs who responded to this survey have been working in state privacy for several years now. But there are many states still lacking a privacy officer. We asked CPOs what advice they would give to those states—or to states looking to elevate the role. Here are the themes.

Clear Authority and Executive-Level Placement Are Essential

Across responses, CPOs stressed that the role must have **explicit authority** and be positioned **high enough in government** to act independently, require agency coordination and endure across administrations.

Privacy Should Be Treated as a Governance and Trust Function — Not Buried in IT or Legal

Respondents consistently warned against structuring the role in a way that reduces privacy to **technical compliance or legal advice**, emphasizing instead its role in **governance, accountability and public trust**.

Statewide Coordination, Resources and Cross-Functional Partnerships Drive Success

Many respondents emphasized that authority alone is insufficient without **funding, staffing, training and strong collaboration** across CIO, CDO, CISO, legal, risk and agency teams.

On the Horizon: How the CPO Role will Evolve

Given the speed of technology and AI, and the privacy implications of these two things, we also wanted to know how state CPOs see their role evolving over the next three years. Across responses, **AI is the single most frequently cited force shaping privacy's future**. Privacy as a priority, an issue and a discipline is increasingly being discussed through an AI lens—sometimes as an enabler, sometimes as an afterthought. Some respondents see AI elevating privacy's importance, while others worry it will crowd privacy out rather than advance it as a discipline in its own right:

> "We have seen and will continue to see a heightened focus on privacy as a result of AI…I expect to see increased attention to privacy in the AI context."

> "Honestly, I see AI crowding privacy out of the conversation and not much progress on privacy."

"With AI now coming into play, it's a bit up in the air… it will be more involved and a much larger part of what the state has to contend with on an annual basis."

"AI will continue to present widespread challenges."

Several respondents describe a shift away from privacy as a narrow compliance function toward **privacy as a data governance and design discipline**, embedded earlier in systems, architecture and decision-making. More mature programs are explicitly pushing privacy "upstream" into data governance, architecture and enterprise risk management. CPOs told us:

"Inventory and classification of data will drive data privacy forward."

"I see privacy in our state evolving from a compliance-focused function into a core data governance discipline."

"Privacy will serve as the organizing framework that aligns legal authority, purpose limitation, minimization, transparency and accountability."

"Deeper integration of privacy in enterprise resource management and architecture."

Many responses highlight that privacy progress depends heavily on **formal authority, role clarity and executive support**, all of which can be fragile, especially during leadership transitions:

"I really hope we are able to have statutory authority to require agencies to implement basic privacy requirements."

"Our program is just roughly one year old…I see a shift in cultural awareness, technological adoption and potentially legislative changes."

"Given that this is an election year and the governor is leaving, it is unclear what the new gubernatorial administration's priorities or support will be with respect to privacy."

NASCIO Recommendations

Based on survey data and advice from state CPOs, NASCIO has the following recommendations for states looking to formally establish a chief privacy officer role or advance the effectiveness of a current CPO:

1. **Ensure dedicated funding.** This year, a lack of funding was the CPOs' biggest challenge and adequate funding was their biggest need. States hold more personal information about citizens than any single private company. Chief privacy officers are tasked with protecting that information and ensuring that states comply not only with privacy laws, but best practices to prevent data leaks. Additionally, today, more than ever, CPOs are becoming experts on AI governance as it relates to privacy. They have big jobs and very few have the budget they need.

2. **Support the privacy program.** CPOs were loud and clear this year—after funding, what they need is support. They specifically asked for support from the state CIO and support of the governor or other senior state management leaders. When you get buy-in higher up, often with that comes budget, authority and enforcement ability. There is still a lot of confusion and lack of understanding in state government about what privacy is. CIOs and other state government leaders can work to communicate to agencies not only what privacy is, but why it's important.

3. **Establish authority and enforcement abilities.** Lack of authority was a top challenge this year and enforcement ability was a top need. Giving state CPOs the authority and enforcement ability to do their jobs will result in a state with a better overall privacy posture. One important way to give CPOs authority is to put the position high enough in government to oversee the enterprise. When the role is embedded too far down into an agency, the CPO can often feel like they are fighting for visibility, which puts privacy in low-priority position.

4. **Expand training and awareness.** A lack of understanding and persistent confusion among state employees emerged as a top challenge for state CPOs this year. Although 46 percent of CPOs report that their states offer mandatory or optional privacy training, many are still working to establish or scale these programs. Strengthening budgets, clarifying authority and increasing executive support would enable more states to launch and expand effective privacy training and awareness initiatives. Training not only improves the work of the CPO, it's an important part of risk management for the state and helps protect the personal information of citizens and employees.

The Future of Privacy in States

State chief privacy officers are becoming enterprise risk leaders operating at the intersection of governance, technology and public trust. As AI accelerates and states manage unprecedented volumes of sensitive data, privacy cannot remain an unfunded mandate or a secondary consideration. The findings in this report make one thing clear: where CPOs have authority, executive support and resources, privacy programs mature quickly and deliver measurable value. The next phase of state privacy leadership will depend not only on laws and frameworks, but on sustained investment, cross-functional collaboration and a shared commitment to protecting the public's trust in digital government.

Primary Author
Amy Glasscock, CIPM
Program Director,
Innovation and Emerging Issues

aglasscock@NASCIO.org

NASCIO
Representing Chief Information Officers of the States

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and technology executives and managers from the states, territories and District of Columbia. NASCIO's mission is to advance government excellence through trusted collaboration, partnerships and technology leadership. 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.