The Shifting Privacy Paradigm

State Chief Privacy Officers' Evolving Roles and Persistent Realities

March 2024

NASCIO®
Representing Chief Information Officers of the States

The Shifting Privacy Paradigm: State Chief Privacy Officers' Evolving Roles and Persistent Realities

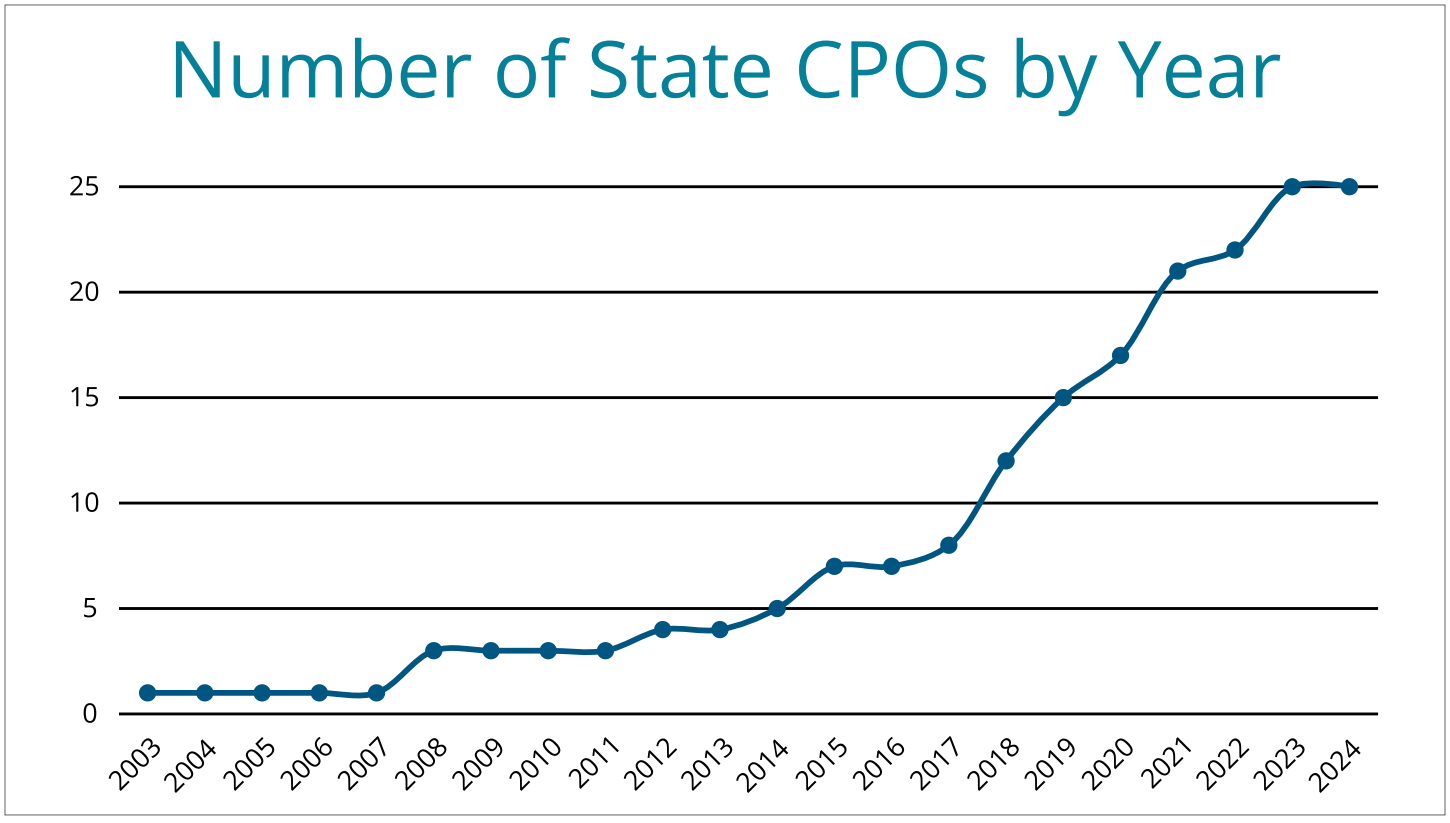
Much has changed in the two years since the last state chief privacy officer (CPO) survey in 2022—and the state of the world has drastically changed from the time of our first survey in 2019! As a policy priority, privacy is continuing to gain in importance for several reasons.

Notably, **the federal government has not passed a comprehensive privacy bill** which has motivated states to pass their own legislation (13 at the time of this publication). A slew of additional states are considering bills this year.

States are also considering **the implications of artificial intelligence (AI)** which has been pushed along by the emergence of generative AI, and are therefore developing comprehensive AI road maps, policies and bills. A large part of the governance of AI includes privacy considerations and state chief privacy officers are finding that they are increasingly involved in this process.

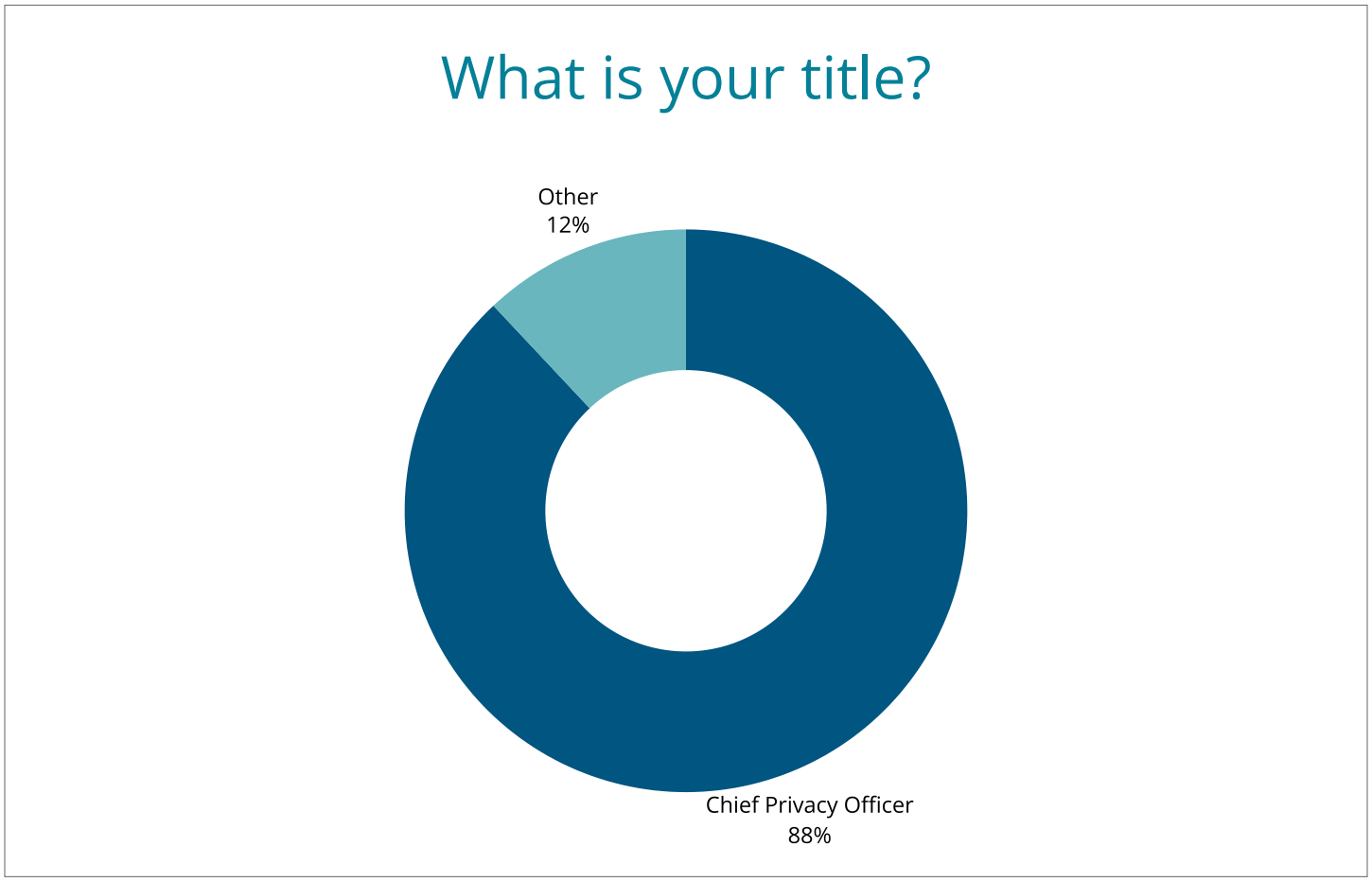
Digital government services are a top priority for state CIOs (it tied with cybersecurity for the number one spot in our State CIO Top Ten Policy Priorities list for 2024). With increased digital services come increased data collection and states want to take the privacy of that data seriously. With this mounting pressure to address privacy at the state level, states continue to hire and elevate state CPOs as we see in this year's survey data.

At the date of this publication 25 states have a chief privacy officer or someone tasked with privacy at the enterprise level (though not all positions were filled) and 17 of them filled out our survey.



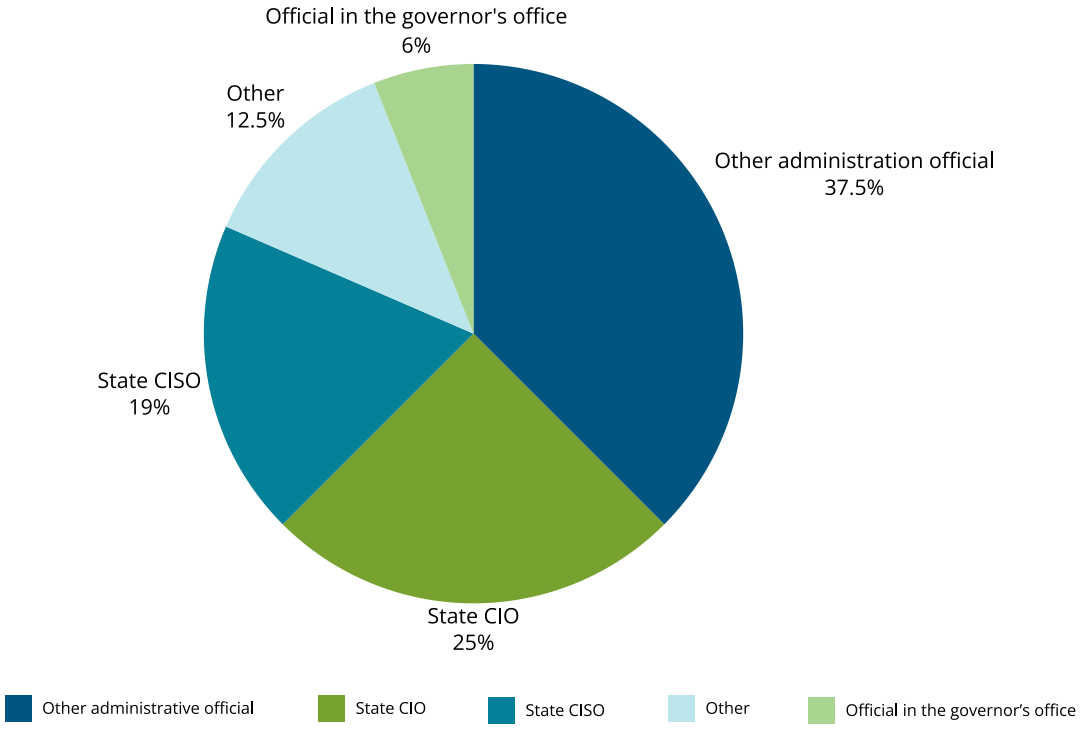
Structure

The title "chief privacy officer" is continuing to become more common as the role becomes more established in states. In 2019, 58 percent of CPOs had the chief privacy officer title (or some similar variation of it), in 2022 it was 65 percent, and today it is 88 percent. Other CPOs have the title added to another title such as general counsel or deputy general counsel, but this increase is a reflection of the importance of the role. We are seeing some states hire an official chief privacy officer after having someone else cover the role part-time, which doesn't add to our overall state CPO count, but shows the role is becoming more established.



As we have in the last two surveys, we asked about the state CPO reporting structure. This year the percentage of CPOs reporting to a state chief information officer (CIO) or a state chief information security officer (CISO) decreased. In 2024, 25 percent of state CPOs reported to the CIO, versus 29 percent in 2022 and 42 percent in 2019. This year 19 percent report to the CISO. That number was 24 percent in 2022 and 33 percent in 2019. This year, the most common answer to the question "To whom do you directly report?" was "other administrative official" at 37.5 percent, showing that the reporting structure is varied across state government and spreading out more as the years go by. This is likely because as the role matures, the importance of privacy is better understood across state government and not just as a function of technology. Privacy may also be starting to stand apart more from cybersecurity instead of being seen as a subset of it.

To whom do you directly report?

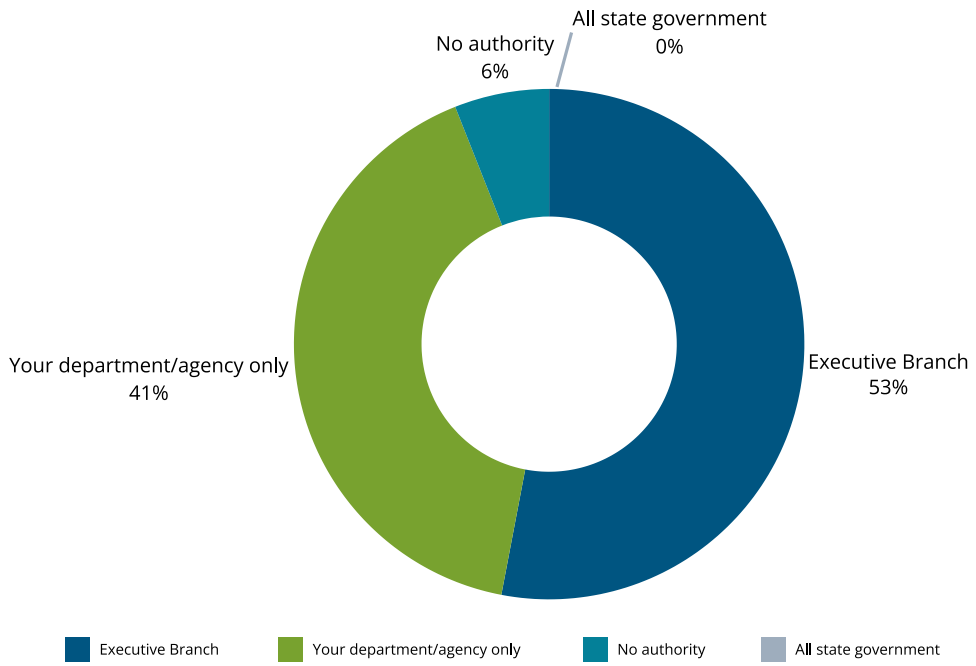


Thirty-five percent of respondents said that they have privacy staff that report to them. Of those that do have staff some of the titles are:

- Deputy privacy officer
- Assistant general counsel
- Privacy analyst
- Privacy and data protection manager
- Privacy fellow
- Director of privacy

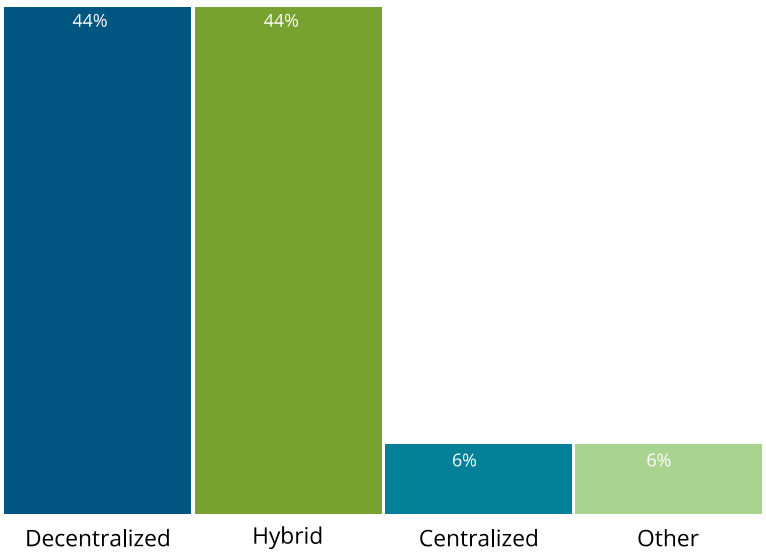
We wanted to know if state CPOs' authority is changing and we asked if they have authority over the executive branch agencies, all state government (including legislative and executive branch) or their department/agency only. Fifty-three percent said that they have authority over the executive branch—the same number as in 2022. Nobody said they had authority over all of state government which is to be expected.

Over which of the following do you have authority?



For the first time, this year we asked respondents if they considered privacy in their state to be centralized, decentralized or hybrid. An equal number were split between decentralized and hybrid (44 percent for each) and only six percent chose centralized.

What is your privacy structure?



Experience and Background

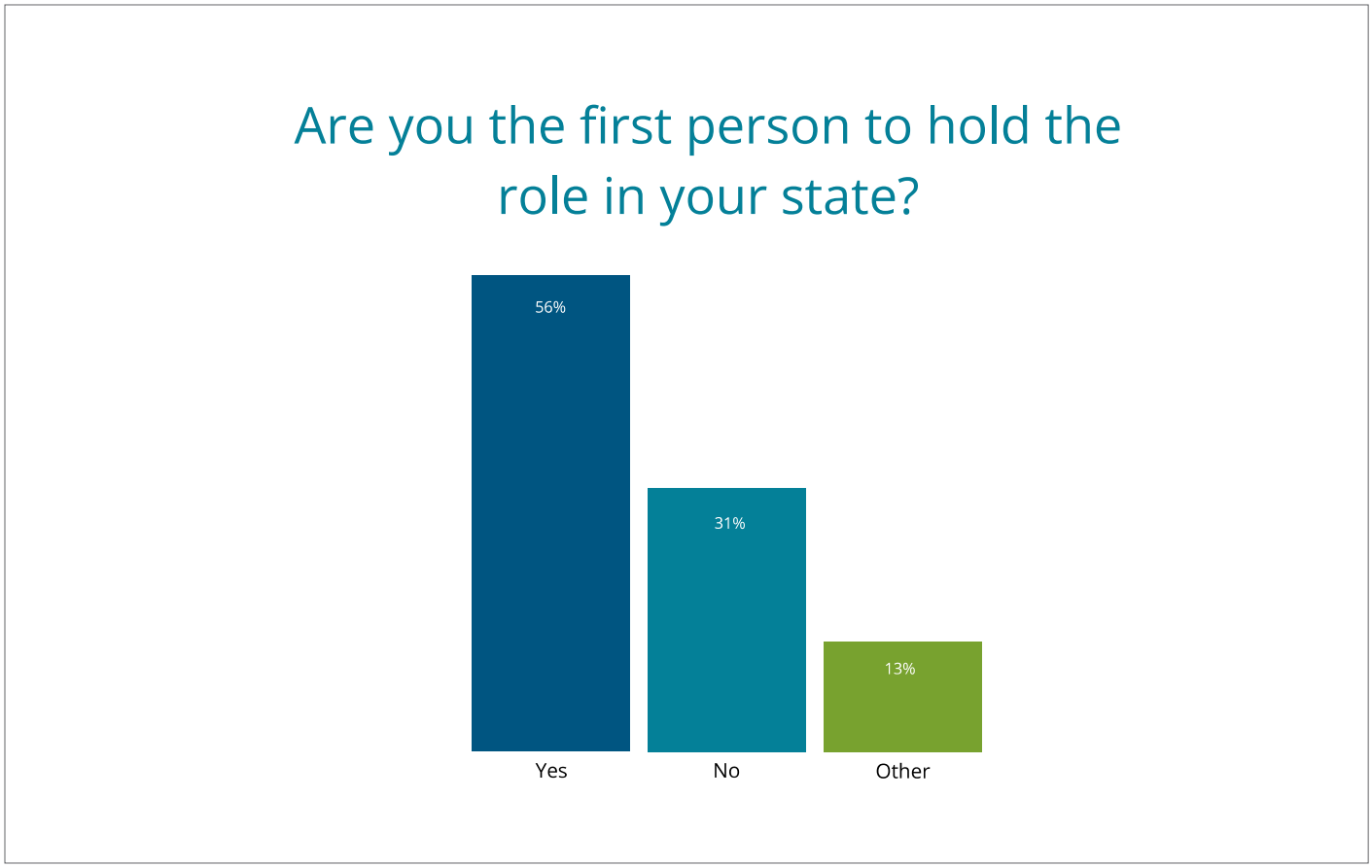
The percentage of chief privacy officers with law degrees was the same this year as it was in 2022--75 percent, but the number of CPOs with privacy certifications rose. While only 76 percent reported having a certification in 2022, this year 88 percent reported a certification with the majority of that number (80 percent) holding a Certified Information Privacy Professional (CIPP) certificate from the International Association of Privacy Professionals (IAPP).

We asked CPOs what professional experience they had before becoming a chief privacy officer. Answers included legal, regulatory, policy, cybersecurity and technology as well as broader privacy or general counsel experience. Several mentioned working on privacy in other state agencies or other levels of government before their current role.

Increasingly Established

This year we saw the number of roles in statute stay the same as it was in 2022—five. We do know that other states have tried to get the role established in statute but were unable to, and we expect the efforts to continue as part of privacy legislation over the next several years.

We again asked each respondent if they are the first person to hold the position in its current iteration and we have seen some fluctuation. In 2019 that number was 67 percent, in 2022 it was down to 41 percent and this year it's back up to 56 percent. While the position has been around long enough that several states have now been through multiple CPOs, the number of states with a CPO for the first time continues to grow and we can see that in this higher number this year. This number will likely fluctuate over the next decade until all states have the role filled.



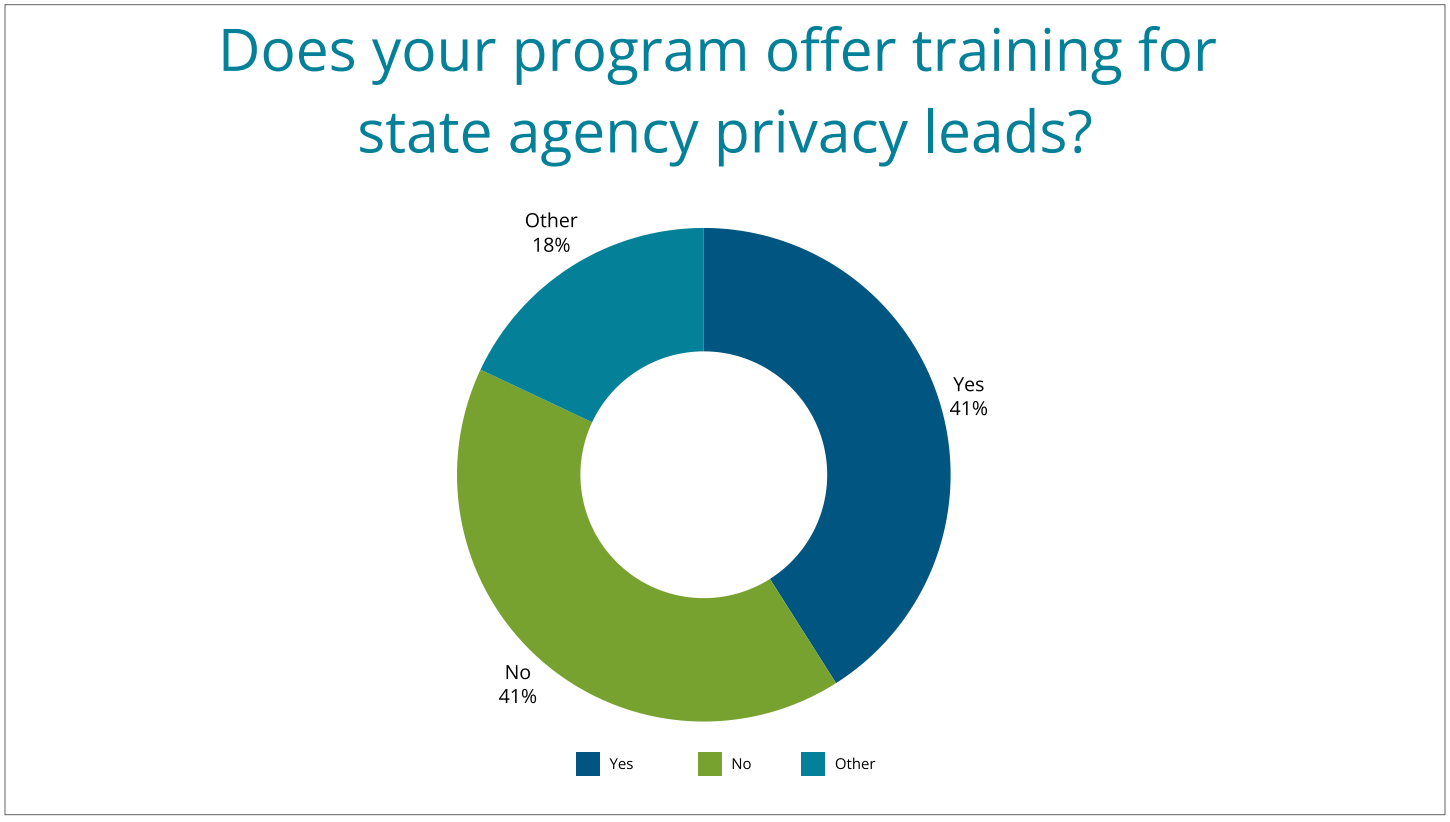
Privacy Program Maturity

We asked CPOs if there is an established privacy program in their state. Twenty-four percent said yes, 41 percent said they are in the process of developing it and 35 percent said no. Oddly these numbers are slightly worse than they were two years ago when 29 percent of respondents said they had an established privacy program. While it remains a priority for states, it seems many are still struggling to establish a privacy program—we learn more about challenges and resources needed below. It's also possible that with so many choosing the "in process of developing option" that some CPOs may feel like the program is just not mature enough to be considered "established" even if they do have an active privacy program.

We asked what privacy framework states follow and only four respondents answered this question. Three states said they use the NIST Privacy Framework, and one follows privacy by design principles. One of the states also mentioned that they follow Fair Information Practice Principles. Frameworks measure and improve an organization's privacy program, and NASCIO recommends that all states use one.

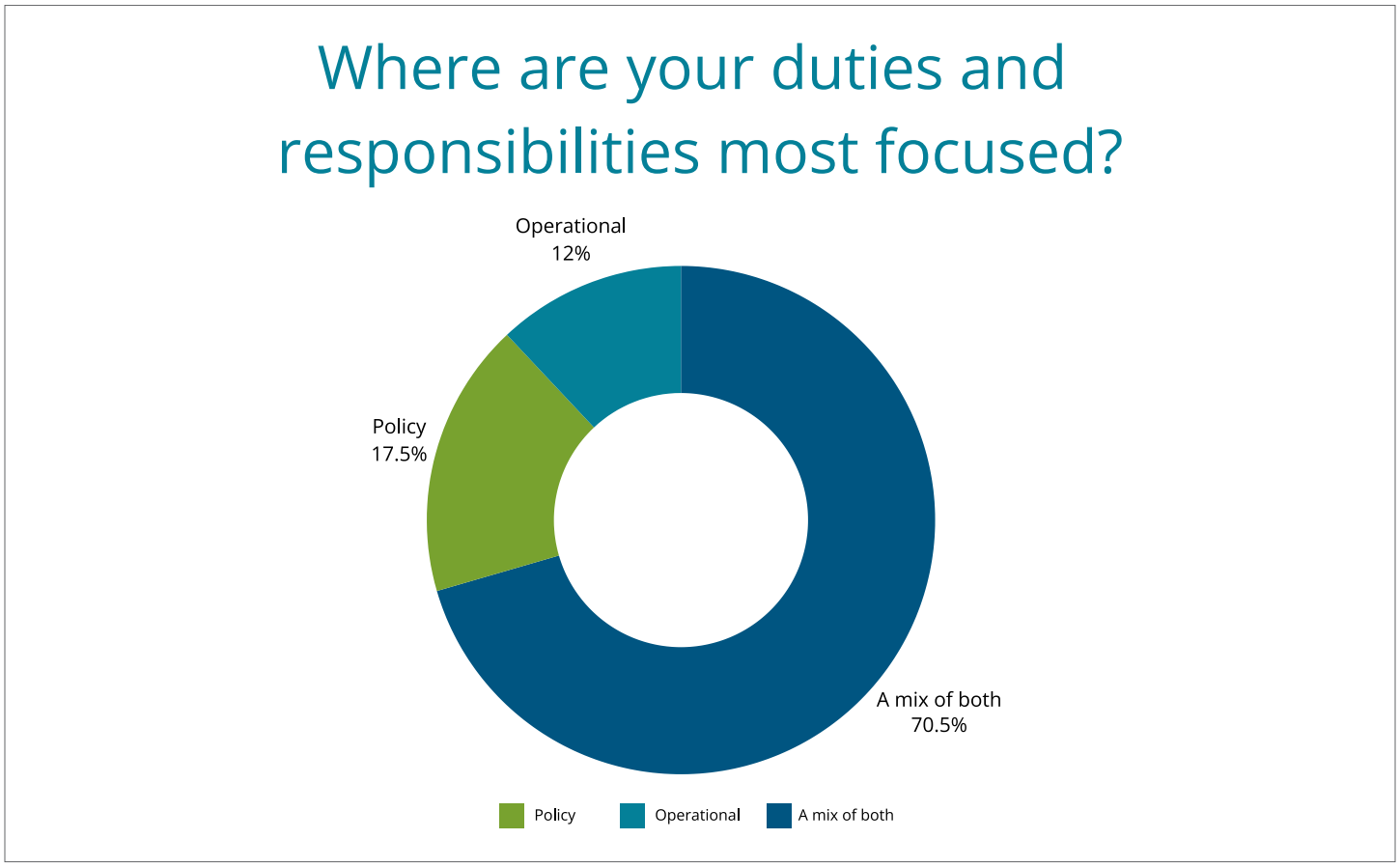
The states that follow a framework said that they have implemented or operationalized the framework by establishing, training and certifying points of contact in each agency; conducting privacy impact assessments; developing privacy rules, policies, statements and guidance; conducting state-wide privacy training; implementing data sharing programs; developing a state privacy framework; and implementing data mapping and governance.

For the first time this year we asked respondents if their privacy program offers training for state agency privacy leads and 41 percent do. Over the last couple of years NASCIO has heard from several states that have started implementing this. It was also a recommendation in our 2022 state CPO survey and report. While 41 percent are not offering training, a few other states said they are either developing it, encouraging it or requesting it. Of the states that are providing training most provide either training from IAPP, internal training or a mix of both. The cadence of training varies from monthly to annually, though most respondents said they offer training on an annual basis.



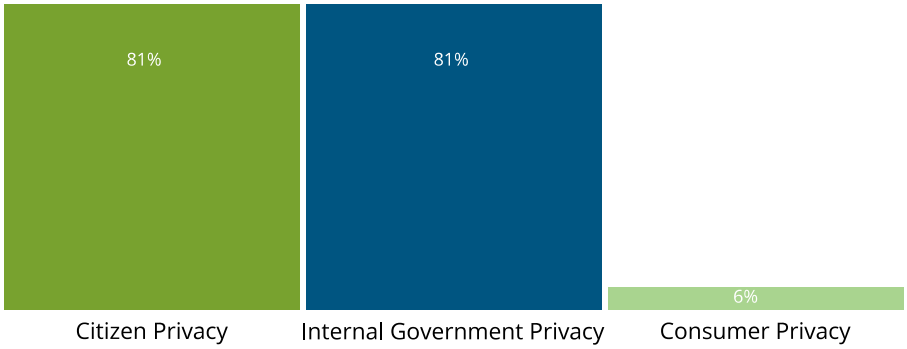
Duties and Responsibilities

We wanted to know what kinds of work takes up the day of the state CPO and asked if their duties and responsibilities are more focused on policy (planning, business strategy, enterprise architecture, policy formation and budgeting), operations (responding to incidents and training) or a mix of both. Not surprisingly the majority of state CPOs focus on both policy and operations, though three chose mostly policy and two chose mostly operational.



We also asked state CPOs if their duties and responsibilities include citizen privacy (protecting the privacy of citizens), internal government privacy or consumer privacy (protecting the privacy of consumers of private businesses). Respondents were able to choose all that applied. Citizen privacy (81 percent) and internal government privacy (also 81 percent) were the most common choices with consumer privacy only at six percent.

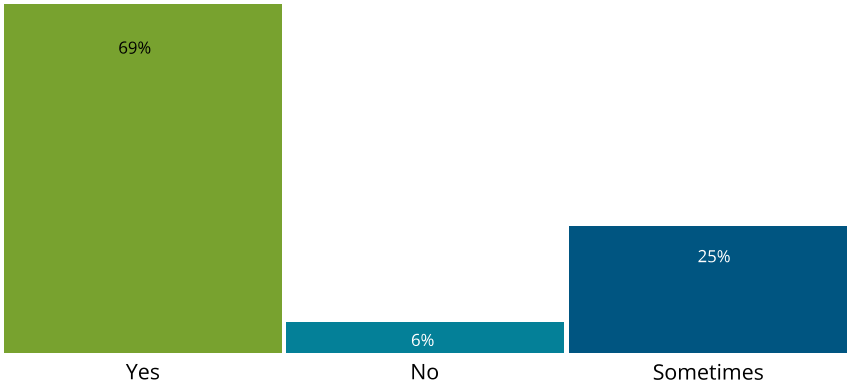
What type of privacy are you most focused on?



Given the explosion of accessibility of artificial intelligence tools over the last year, we asked state chief privacy officers if they have been involved in setting policies related to artificial intelligence for their state. A resounding 77 percent said that they are while only 23 percent said that they are not. AI and privacy are converging right now in a way we have not seen in the past. IAPP, an organization mainly focused on privacy, has rolled out an AI governance certification and privacy professionals are increasingly sought out for their critical input when it comes to AI governance and policy setting.

Along with the increased interest in AI comes more questions around privacy as it relates to technology procurement and acquisition. A full 69 percent of respondents said that they are involved in the approval process for technology-related procurements and contracts (compared to 59 percent in 2022) and 25 percent said that they are sometimes or in certain situations. This growth likely shows the increasing importance of considering privacy in the procurement process. Of note, only one CPO reported ***no*** involvement in technology-related procurements.

Are you included in the approval process for technology-related procurements and contracts?



Finally, we asked what tools state CPOs are using to standardize and automate privacy tasks. The most popular answers were privacy impact assessments at 53 percent and risk management at 53 percent.

Authority and Budget

Absence of a defined budget and lack of authority are always pain points for state CPOs. Lack of funding and authority prevent them from fully implementing the state privacy programs that are needed across the nation and we hear this each time we conduct a survey.

This year three states said that they have a defined budget for privacy initiatives compared to only one state in 2022. Two other states mentioned that while they don't have a defined budget for privacy specifically, there is money available for privacy in other budgets. Of the defined budgets for privacy, they range from $3 million a biennium to $2 million a year and come from appropriations, grants and agency allocations.

Only 20 percent of state CPOs report that they have the authority to enforce compliance with enterprise privacy policies compared to 42 percent two years ago. Twenty-seven percent said privacy policies are enforced by another entity, and another 27 percent said that privacy policies are not enforced. One respondent said that while they do have legislative authority, in reality, the ability to enforce the policies can be challenging. We don't know why this number went down, but with a small number of respondents each year it's easy for the numbers to vary if a couple of CPOs interpret their authority differently than someone who filled out the survey in past years.

Challenges and Resources

As we have each year, we asked state CPOs to choose their top three challenges in their state for improving privacy practices. The top three answers were lack of authority given to the state CPO, lack of funding for privacy initiatives and lack of qualified staff. A close fourth was lack of understanding among state employees / confusion which was in the top three in 2022.

Lack of authority

Lack of Funding

Lack of Qualified staff

We also wanted to know about the top five items or resources that state CPOs need to do their job effectively. The top five answers were an effective privacy governance structure, adequate funding, support of the governor or other senior management leaders, adequate staffing/personnel and support of state agencies.

Privacy Governance

Funding

Governor's Support

Staffing

Agency Suport

Advice to States

Each year we hear from new states that are ready to hire a chief privacy officer for the first time and they ask NASCIO for advice on how to structure the role. In each of our state CPO surveys we like to gather information from current state CPOs to find out what works best in their states. Here are some of the things we heard this year.

The CPO needs the proper **authority** to do their job effectively and report to a high level. Some respondents suggest that the role be appointed by the governor and under the governor's office or at least reporting to the CIO or higher level. This ensures visibility to perform the necessary privacy functions.

Several suggested that the role be **established in statute with a defined budget and staff** to prevent it from being easily eliminated. We hear over and over from state CPOs that they struggle to implement privacy practices with no funding.

Another common theme was the importance of having **privacy analysts designated at the agency level** to assist with the day-to-day execution of the privacy program. This also ensures that state agencies are all on the same page with respect to privacy.

Advice to a New State CPO

We also wanted to know what wisdom sitting CIOs can impart on new ones. Here is some of the advice we received.

Connect with other state CPOs.

"Join NASCIO forums to connect with your peers. It's a great opportunity to hear from your colleagues in other states about what they're doing, where they've been successful and how to overcome challenges they may have already faced."

"There are lots of states now with active privacy programs. Look to those state CPOs for guidance, see what works for them and how you may incorporate it into your state."

"Connect with other states. Share resources, no need to reinvent the wheel."

Build relationships.

"Build relationships and learn where existing programs like legal, IT, security, procurement and compliance have levers in the IT contracting process and IT development lifecycle. Leverage those as opportunities to incorporate privacy and do so in accordance with a recognized standard."

"Ensure your agencies view you first and foremost as a resource and be accessible to them."

"Work closely with the CIO and CISO."

Turn limitations into opportunities.

"Reach out to the CPO community, get a CIPP certification, recognize that there are lots of federal resources that can help and anticipate that you may be without help or funding for longer than you expected."

"Establishing program, process, policies, procedures and buy-in takes time."

"Focus on incremental improvements that will be long lasting. Privacy is too important to not get right, and in government, privacy needs to be operationalized in a way that it will exist and function with CPO turnover."

Recommendations

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

1. **Establish privacy governance.** The number one thing that state CPOs said they need to do their job effectively this year was an effective privacy governance structure. Only four CPOs reported that they follow a privacy framework, however all states should follow a privacy framework (such as NIST). Having a privacy governance structure and working privacy into the enterprise architecture of the state is important for elevating privacy, organizing privacy within the enterprise and giving authority to the CPO and the privacy program. A framework supports the governance of the privacy program and can help the privacy team develop a common language with the security team which many in government are already familiar with.

2. **Ensure dedicated funding and authority.** Lack of authority given to the state CPO was the number one challenge reported this year. CPOs cannot effectively do their work if they are embedded too far down in state government. Additionally, a privacy program without adequate funding also prevents a program from being effective. Lack of dedicated funding was also a top challenge and needed resource for state CPOs. Given that only three states reported having a dedicated privacy budget, this is something that is needed not only by future state CPOs, but current ones as well. The budget should include funding not only for privacy initiatives, but also for dedicated privacy staff.

3. **Establish and train agency leads.** Whether through legislation, executive order or policy, a privacy lead should be established at each agency. This ensures that the CPO has help understanding the lines of business and there is someone to champion privacy at the agencies. If finding qualified privacy staff is a challenge, states can take the lead from other states who are training existing staff through IAPP or internal programs, ensuring they possess the necessary expertise.

Primary Author/NASCIO Contact

Amy Glasscock

Program Director,
Innovation & Emerging Issues

NASCIO

aglasscock@NASCIO.org

About NASCIO

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. For more information, visit www.NASCIO.org.