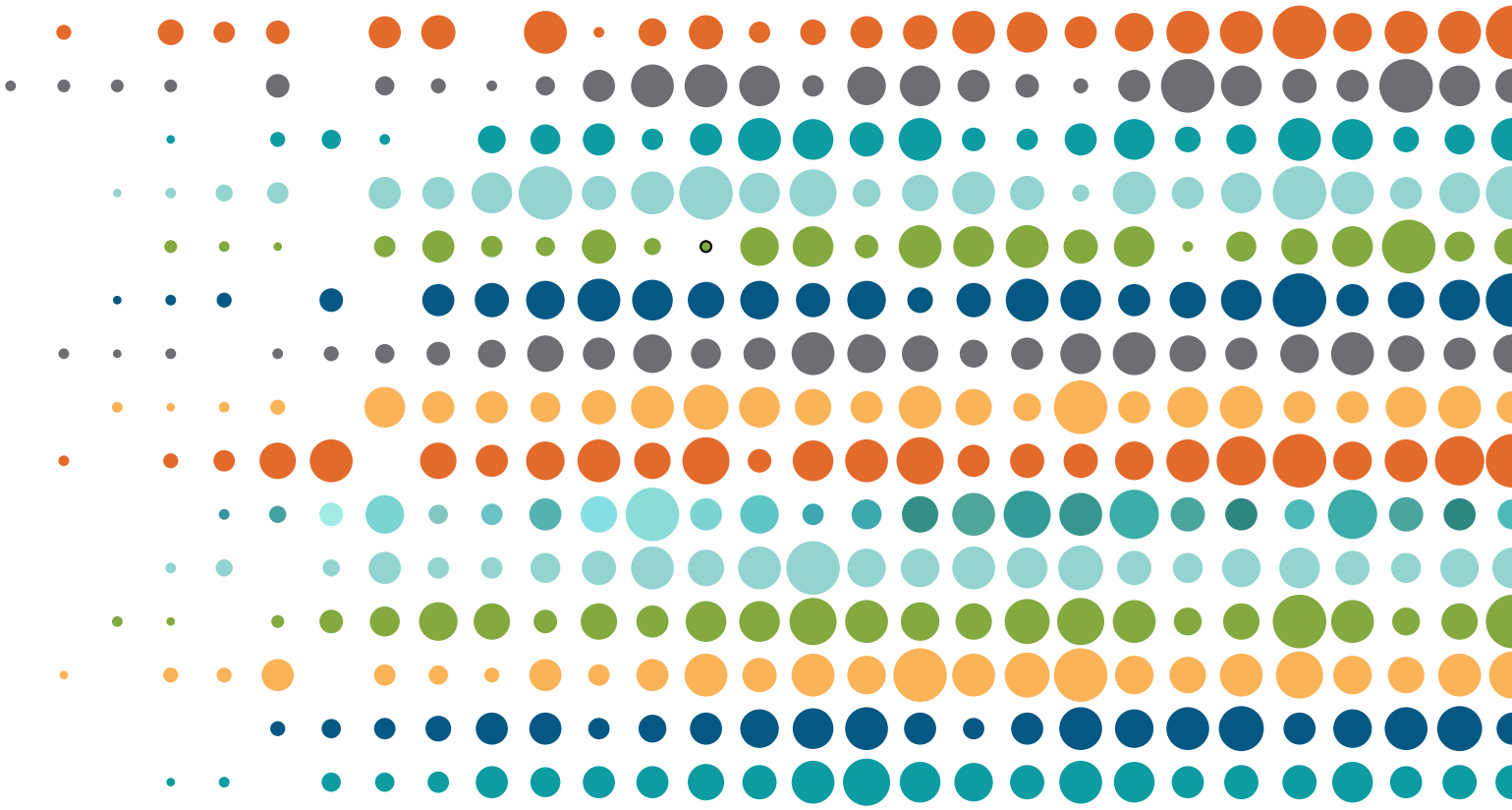
Privacy Progressing

How the State Chief Privacy Officer Role is Growing and Evolving

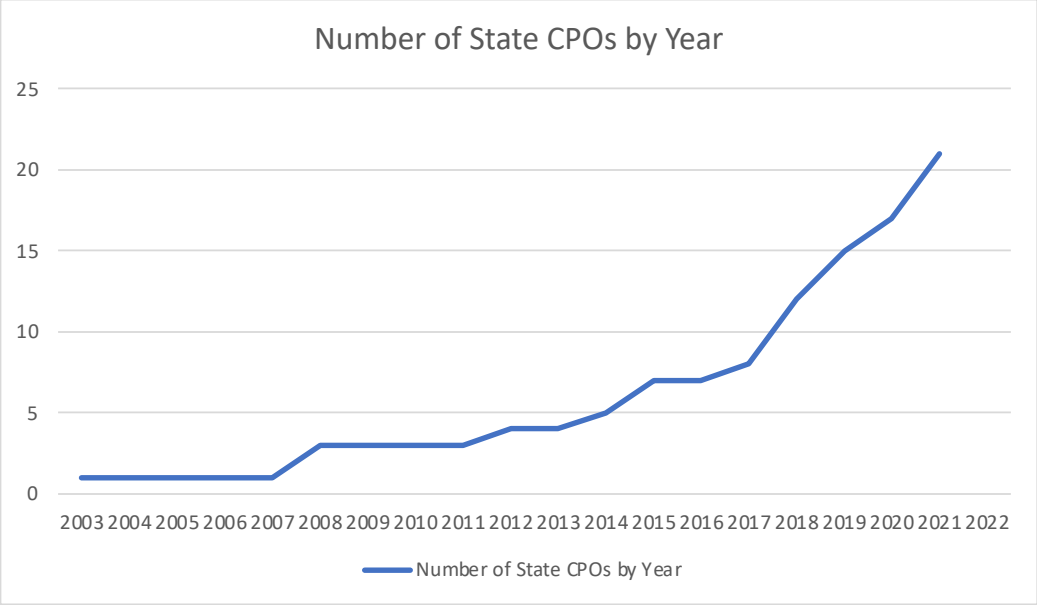
June 2022



NASCIO®
Representing Chief Information Officers of the States

In the last decade there has been immense growth in the state chief privacy officer (CPO) role. As demand increases for online services and states capture more personally identifiable information from citizens, more states are emphasizing the importance of privacy. In addition, citizens are becoming more aware of privacy rights, and more concerned about how government might be handling their information. According to Pew Research, 60 percent of U.S. adults believe it's not possible to go through daily life without having data collected about them by companies or the government.

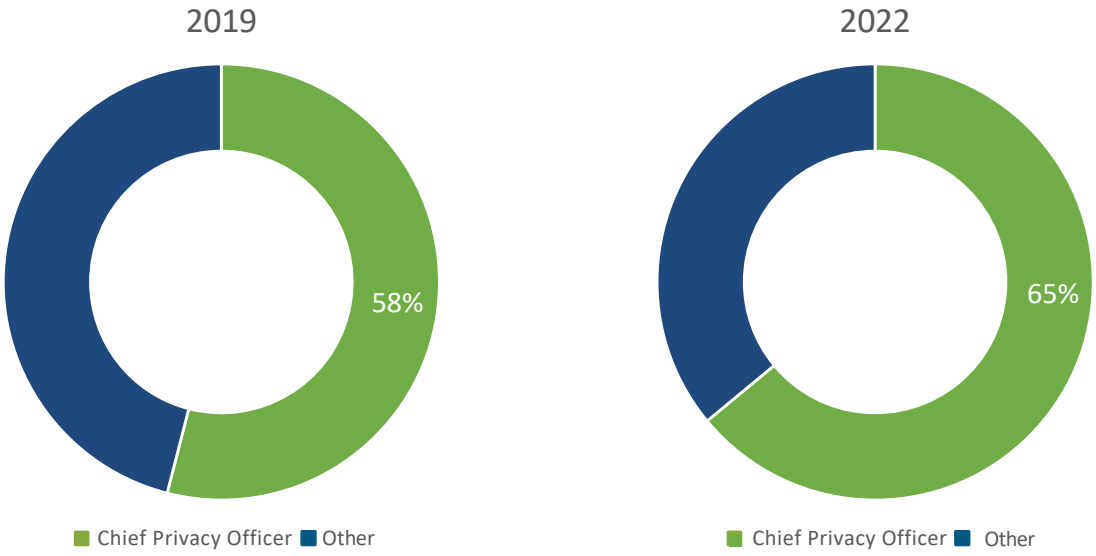
NASCIO first wrote about the state chief privacy officer (CPO) role in 2019 with the report, "Perspectives on Privacy: A Survey and Snapshot of the Growing State Chief Privacy Officer Role." At the time that report was released, twelve states had identified someone in the CPO role. Just three years later, 21 states have the state CPO role (or at least someone who leads privacy at the enterprise level). As the number of state CPOs grows, we wanted to check in with this group to see how the role is evolving, growing and settling into the structure of state government.



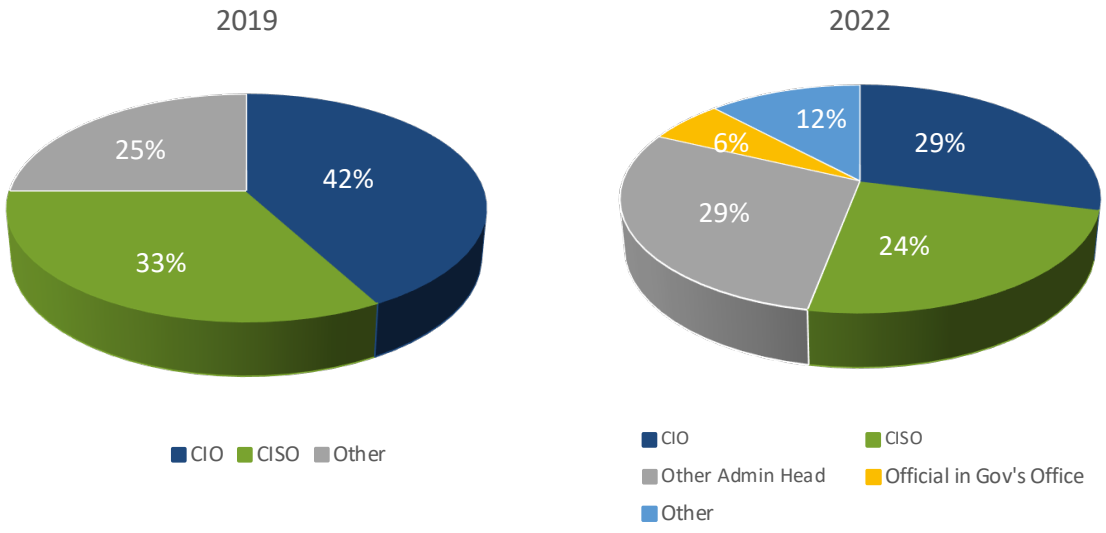
At the time of this survey, 20 states had the CPO or equivalent position filled and one state had the position, but it was not filled. Out of the 20 with the position filled, 17 responded to our survey.

Structure

When we asked state CPOs about their title, not surprisingly, as the role becomes more common and established, more privacy officials doing this job have the title "chief privacy officer" or some variation of it. The second most popular title was "general counsel" or some variation of that. In 2019, 58 percent of CPOs had the chief privacy officer title, and today 65 percent have the title. Twenty-four (24) percent of respondents have the "general counsel" title.

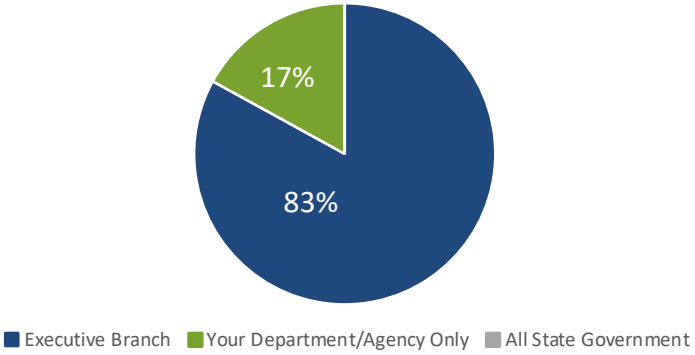


As we did in 2019, we asked state CPOs about their reporting structure. In 2022, 29 percent report to the state chief information officer (CIO), 24 percent report to the state chief information security officer (CISO), 29 percent report to a different administrative head, six percent report to an official in the governor's office and 12 percent chose "other." This is also different from 2019, when 42 percent reported to the CIO, and 33 percent reported to the CISO. The fact that 29 percent report to the CIO in 2022 versus 42 percent in 2019 shows that as the role grows in numbers, the trend of reporting to the CIO is declining. Reporting to the CIO is still more common in state government than it is in the private sector. A 2014 survey from the International Association of Privacy Professionals (IAPP) of Fortune 100 chief privacy officers reported that only 3% report to the CIO. As this role matures, it makes sense that more states are structuring it outside of the technology department. Privacy is important across the enterprise and is tied to security and data, not just technology, and the state CPO should have jurisdiction over the entire executive branch.

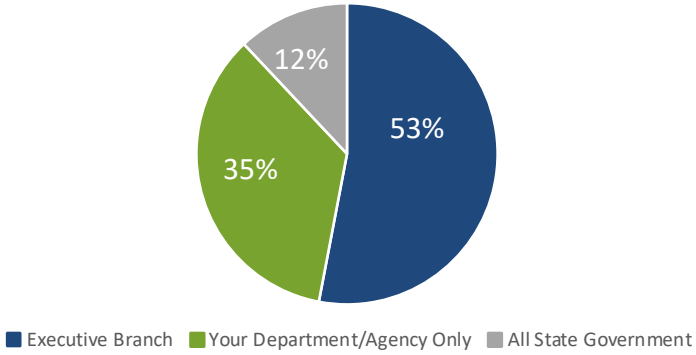


We asked state CPOs about their authority—all state government (executive, legislative and judicial branches), executive branch or their department/agency only. The most popular answer was executive branch with 53 percent of responses, followed by their department/agency only with 35 percent and all state government with 12 percent. This is an interesting change from 2019 when 83 percent of respondents said they had authority over the executive branch and 17 percent over their agency only. No state CPOs reported in 2019 that they had authority over all state government. With a relatively small sample size, and many different people answering in 2019 and 2022 it's hard to say if this decrease in authority over the executive branch is actually a trend—but if it is, it's concerning. NASCIO recommends that the enterprise privacy role have authority over the executive branch. It would be unlikely for many CPOs to have authority over all of state government (though 12 percent reported that they did), but they should at least have a collaborative relationship.

Over Which of the Following Do You Have Authority? (2019)



Over Which of the Following Do You Have Authority? (2022)



Seventy-one (71) percent of state CPOs said that they have staff that report to them, however the ones with the most staff are also serving in a general counsel capacity and may have direct reports that don't focus on privacy.

Examples of the privacy-related direct report positions include the following:

- Privacy officer
- Security and privacy training and awareness coordinator
- Privacy analyst
- Privacy attorney
- Assistant chief privacy officer
- Administrative assistant
- Privacy and data protection manager

Experience and Background

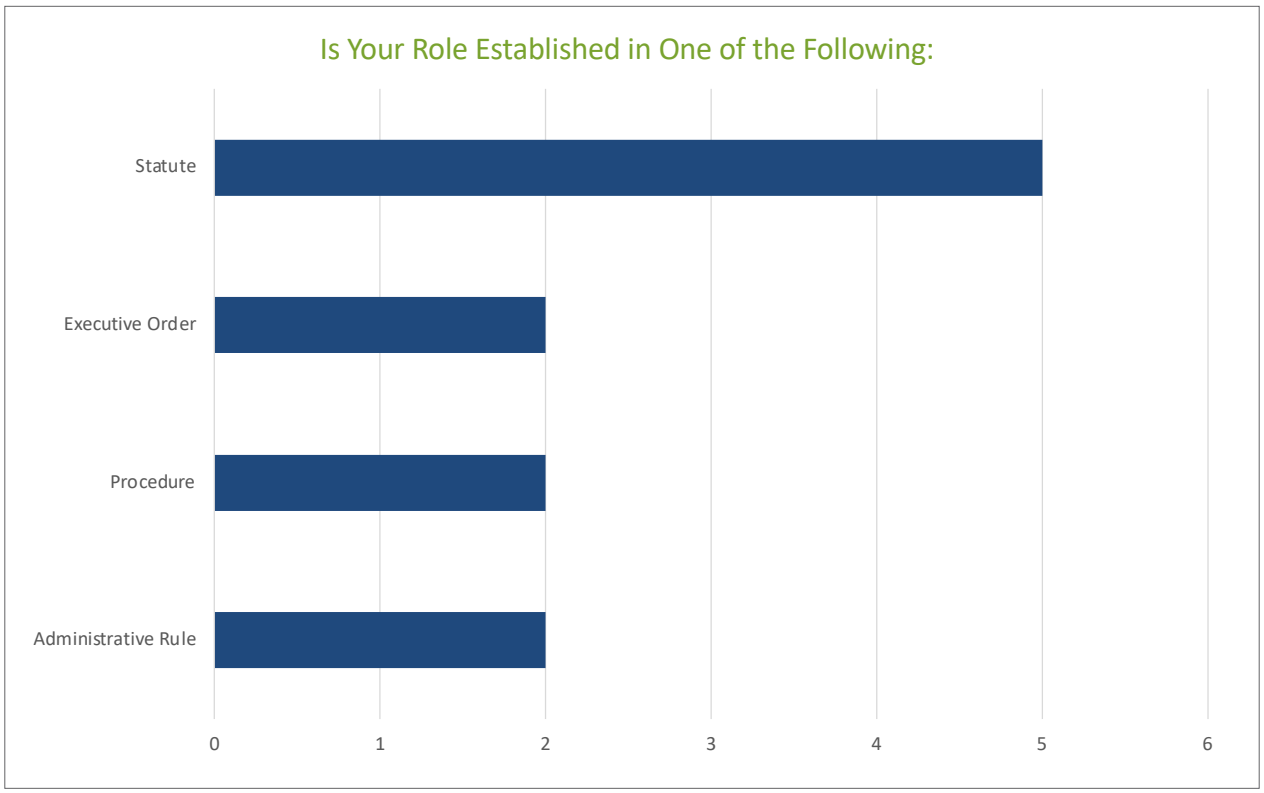
Law degrees continue to be common among chief privacy officers—even more so now than in 2019. This year 76 percent of respondents reported having a law degree, compared to 58 percent in 2019. For those chief privacy officers that do not hold law degrees, they tend to have extensive experience in privacy and security and often government.

Privacy certifications from IAPP are gaining in popularity as well. This year ten CPOs reported having a Certified Information Privacy Professional (CIPP) certification, two reporting having a Certified Information Privacy Manager (CIPM) certification and one is a Fellow of Information Privacy.

This year we asked CPOs about the professional experience that led to their current position. Many mentioned working as attorneys as well as careers working in privacy or security in the public and private sector. Several CPOs mentioned working in specific sectors such as health and human services, regulatory, technology, telecom and contracting—all areas where privacy is a focus.

Increasingly Established

In 2019 only three state CPO positions were established in statute, and a handful were established by executive order. The rest were just listed as part of policies. This year five were established in statute, two by executive order, two by procedure, two by administrative rule and the rest either were not officially established, were part of an organization or mentioned in an official policy.



We can also see the CPO role maturing simply because more states have had the role for longer. In 2019, 67 percent of the CPOs interviewed were the first person to hold the role in their state. This year 41 percent said they are the first person to hold the role (in its current iteration). This shows that more states have had the CPO position long enough now that there has been some turnover. Another 41 percent said they were not the first to hold the position and 18 percent said that even though they are doing the work of a state CPO, they don't consider themselves an official state CPO, so they chose the "other" option.

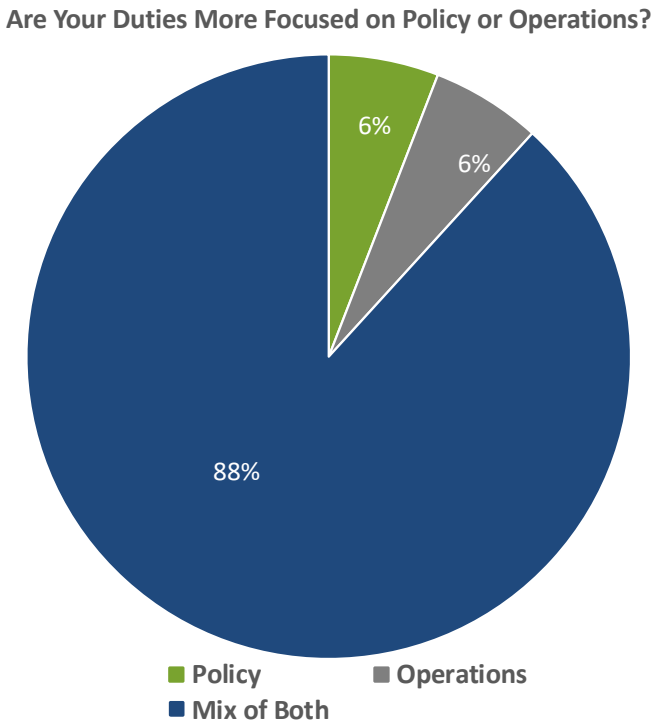
Privacy Program Maturity

When we asked state CPOs if there is an established privacy program in their state, 29 percent said yes, 41 percent said they are in the process of developing it, and 29 percent said they do not have one. With two-thirds of states having or working on an established privacy program, this is clearly a top privacy priority for states.

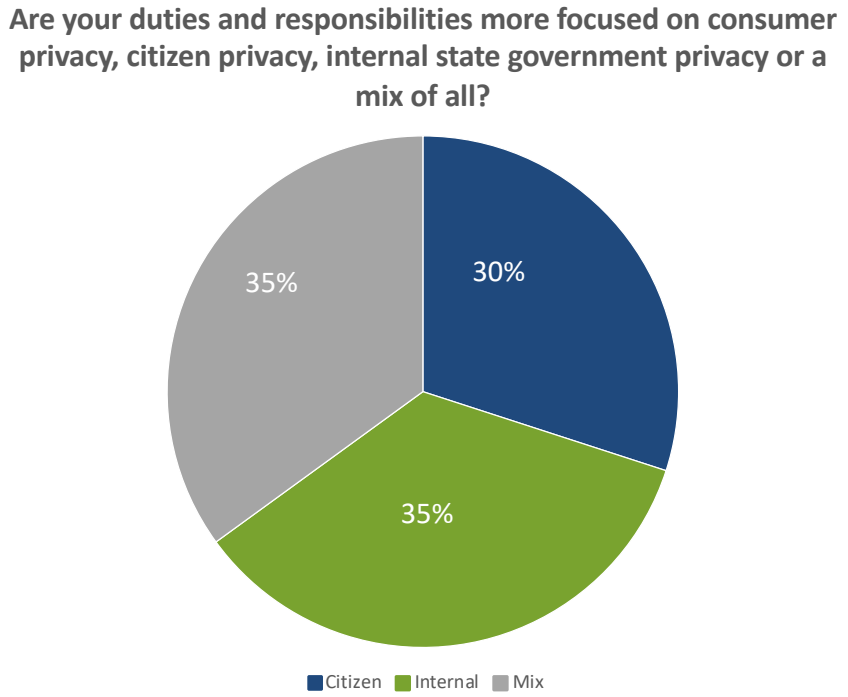
This year we also asked about what privacy frameworks states are following and asked them to choose all that applied. The most popular answer was the NIST Privacy Framework (52 percent) followed by privacy by design (12 percent). Three states said they did not follow any frameworks, and three said they were still in the process of developing a framework. Two states also mentioned following Fair Information Practice Principles in the comments. Frameworks are used to measure and improve an organization's privacy program, and we recommend that all states use one.

We also wanted to know what steps state CPOs have taken to implement or operationalize the framework that they follow. Answers included writing standards, policies and guidelines based on the frameworks; posting policies internally and externally; requiring government applications to go through a governance, risk and compliance tool before moving forward; developing privacy impact assessments and privacy threshold analyses; requiring data classification before file transfers; embedding privacy into policies and processes; developing privacy training; and implementing enterprise privacy policies.

We asked state CPOs if their work was more policy-focused (planning, business strategy, enterprise architecture, policy formation and budgeting), operational (responding to incidents and facilitating training) or a mix of both. The overwhelming majority (88 percent) said a mix of both with just one CPO choosing policy and one choosing operational.



We also asked state CPOs if their duties and responsibilities were more focused on consumer privacy, citizen privacy, internal state government privacy or a mix of all. Unsurprisingly no state CPO chose consumer privacy. Thirty-five (35) percent chose internal state government privacy, 35 percent chose a mix of all, and 30 percent chose citizen privacy. Citizen privacy will continue to be a focus given the high priority on digital services now and in the future. States will need to put an emphasis on citizen privacy to restore and maintain citizen trust with state government.



We also asked state CPOs what they spend the bulk of their days working on. Policy-related duties included developing and revising privacy policies; developing standard language and practices; working with stakeholders to embed privacy into processes; working with cybersecurity and data officials to align policies; and providing guidance to other branches of government.

Operational tasks included responding to incidents; guiding agencies through incident response; increasing privacy awareness; leading trainings; negotiating contracts; directing privacy compliance reviews; overseeing the process for privacy impact assessments; responding to citizen privacy concerns; and drafting data sharing agreements.

We asked state CPOs if they are included in the approval process for IT-related procurements and contracts. Fifty-nine (59) percent said that they are.

Authority and Budget

In the 2019 NASCIO CPO publication, one of the recommendations that came out of the state CPO interviews was the need for established authority to enforce privacy as well as a dedicated budget. This year, we asked state CPOs if they possess the authority to enforce compliance with enterprise privacy policies. Forty-one (41) percent said yes, 35 percent said they are enforced by another entity and 24 percent said they are not enforced. Of those who said they are enforced by other entities, most of those CPOs said they were enforced at the agency level. One respondent said the state auditor is responsible for checking that privacy impact assessments are complete, and another said that the cabinet secretary can enforce via funding approval and administrative directives.

A dedicated budget for privacy initiatives is still a pain point for state CPOs. Only one state responded that they have a defined budget for privacy initiatives. The nearly three-million-dollar budget is from a dedicated appropriation. Most CPOs are getting funding from the IT, security or other agency budget depending on where the role is structured.

Challenges and Needs

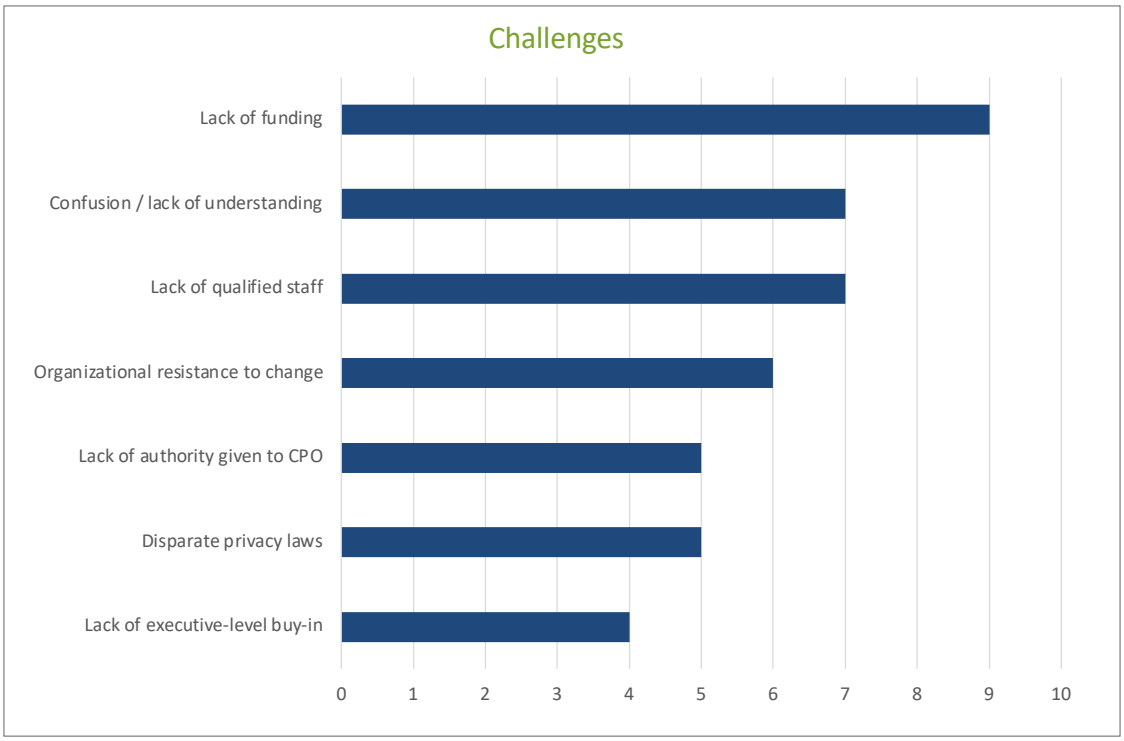
We wanted to know what the biggest challenges are for CPOs in improving privacy practices. We gave seven options, allowing CPOs to choose three, and all got several votes. The three most popular were:

• Lack of funding for privacy initiatives

• Lack of understanding among state employees / confusion

• Lack of qualified staff

Lack of funding and qualified staff are issues we hear about across state IT and pose problems in lots of areas. However, the lack of understanding and confusion challenge is more unique and likely stems from the relatively up-and-coming nature of privacy in state government and the confusion that comes from employees believing that privacy is a subset of security.



We also asked state CPOs to choose the top five items/resources they need to do their job effectively. Out of ten options, all got several votes. The top five were as follows:

- Adequate funding
- An effective privacy governance structure
- Support of the governor or other senior state management leaders
- Adequate staffing/personnel
- Support of state agencies
- Incorporation of privacy into state enterprise architecture

Advice From the Trenches

Often NASCIO hears from a CIO, CISO or other government official looking to hire a state chief privacy officer for the first time, seeking job descriptions or other information on how to structure the role. We asked state CPOs what their advice would be for states looking to develop the CPO position for the first time. The advice was similar to what we heard three years ago:

States really need **executive-level buy-in** before creating the position and the reason for creating the position needs to be clearly stated and developed.

The position needs to have **strong authority and visibility in a centralized location** such as the governor's office, information technology, legal department or department of administration and should have an equal voice to the CIO and the CISO. One CPO stated the importance of the relationship with the information technology agency by writing, "The exact structure of the role and the agency where it resides are likely specific to the needs and vision of the particular state; however, regardless of those factors, there must be a strong nexus with the office or agency providing information technology services."

A different CPO stated, "At a minimum, the CPO should be a functional position and not just a figurehead. Regardless of where the CPO is positioned, they should be able to set policies and standards, and have the ability to enforce those across all departments."

Having **privacy counterparts at the agency level** was also mentioned by several state CPOs. As one stated, "Within the executive order that created my position, other executive agencies were required to designate counterparts to my position at the agency level (i.e., agency chief privacy officer). I would suggest to other states looking to create a state CPO position that these counterparts are important. These other positions help to collaborate and spread the importance of privacy at the agency level."

With new state CPOs coming into the role each year, we asked current CPOs what their advice would be to someone new to the role.

Many state CPOs stated the importance of **building relationships with the CIO, CISO, chief data officer and legal teams**, stressing the importance of close communication and collaboration with these other key positions.

Another good piece of advice is to **understand the needs of the agencies** that you are working with. As one respondent put it, "I would say that they need to collaborate with agency personnel and understand the intricacies of the information that is collected throughout many state agencies. There is a vast difference from agency to agency in terms of how much information they collect, the purpose of collection and the ultimate regulatory or statutory requirements they need to abide by ultimately. Stick to general best practice principles but know that you may have to guide agencies through very unique problems and issues."

Several respondents mentioned the value that can be gained by reaching out to other state CPOs and **getting involved in membership organizations such as NASCIO**. As one state CPO said, "Take advantage of NASCIO resources and forums. Some states have fairly developed programs, so it's a great way to learn what works (and what doesn't)."

More than one state CPO advised new CPOs to **take things one step at a time**. It's hard to build a new privacy program from scratch. As one CPO put it, "Building a privacy program will take many years and will often require the creation of additional laws and administrative rules. Start with a long-term view and be empathetic of the agencies you will be working with. Many of these agencies have never been told to build a robust privacy program. They want to improve; they just need proper guidance and time."

Here are a few other great quotes we got in response to this question:

"Identify a clear scope of responsibility that is complementary to existing roles/functions (e.g., CIO, CISO, CTO, etc.)."

"Create a strategic plan, make stakeholders aware of privacy and that privacy is everyone's responsibility. Review frameworks and use what is helpful, customize it for your needs and the needs of your state."

"Get a handle on what your role is for the state and then build out from that authority. Set a foundation for the privacy program and be willing to engage and understand all perspectives regarding data use. There is a fear from others that the state CPO is there to tell everyone "no" so you need to proactively counter that attitude. Show that you want to help agencies achieve their objectives while taking privacy into consideration - this comes from the 'privacy by design' framework as well."

"My initial advice would be to read and become educated with state IT security and privacy policies, standards and procedures. Meet with agency subject matter experts (HIPAA, IRS Pub1075, CJIS, etc.) and develop a good working relationship with them."

"The IAPP CIPM framework for privacy program management provides a tremendous roadmap for your efforts. Outline the process in the abstract and superimpose your organization's needs onto it; focus on the low-hanging fruit, deliver value and repeat!"

Recommendations

Based on the survey and advice from the 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. **Ensure dedicated funding for a privacy program and staff.** The CPOs' top challenge was a lack of dedicated funding for privacy initiatives and their most needed resource was adequate funding. Given that only one state CPO 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 to support the state CPO.

2. **Establish privacy governance**. 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. In addition states should follow a privacy framework.

3. **Develop agency relationships**. For a state CPO to be effective they not only need to understand the needs of the agencies, but the agencies need to understand the importance of privacy. Have a privacy lead at the agency level—this person will champion privacy to agency employees while providing a direct line of communication to and from the chief privacy officer. If agencies do not have privacy leads, and cannot hire them, look into providing training to create agency privacy leads.

Primary Author/NASCIO Contact

Amy Hille 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.