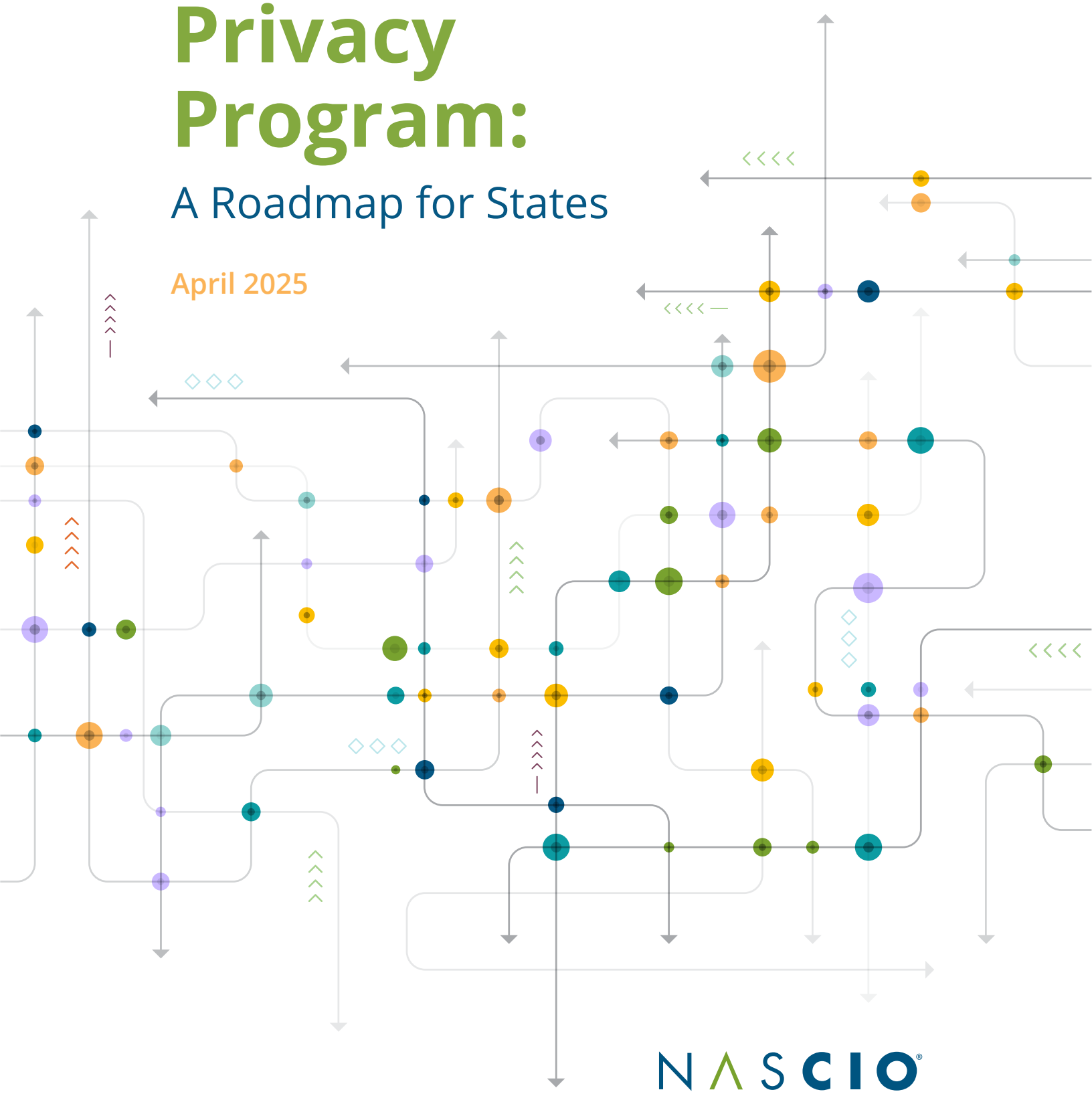
Creating a Privacy Program:

A Roadmap for States

April 2025

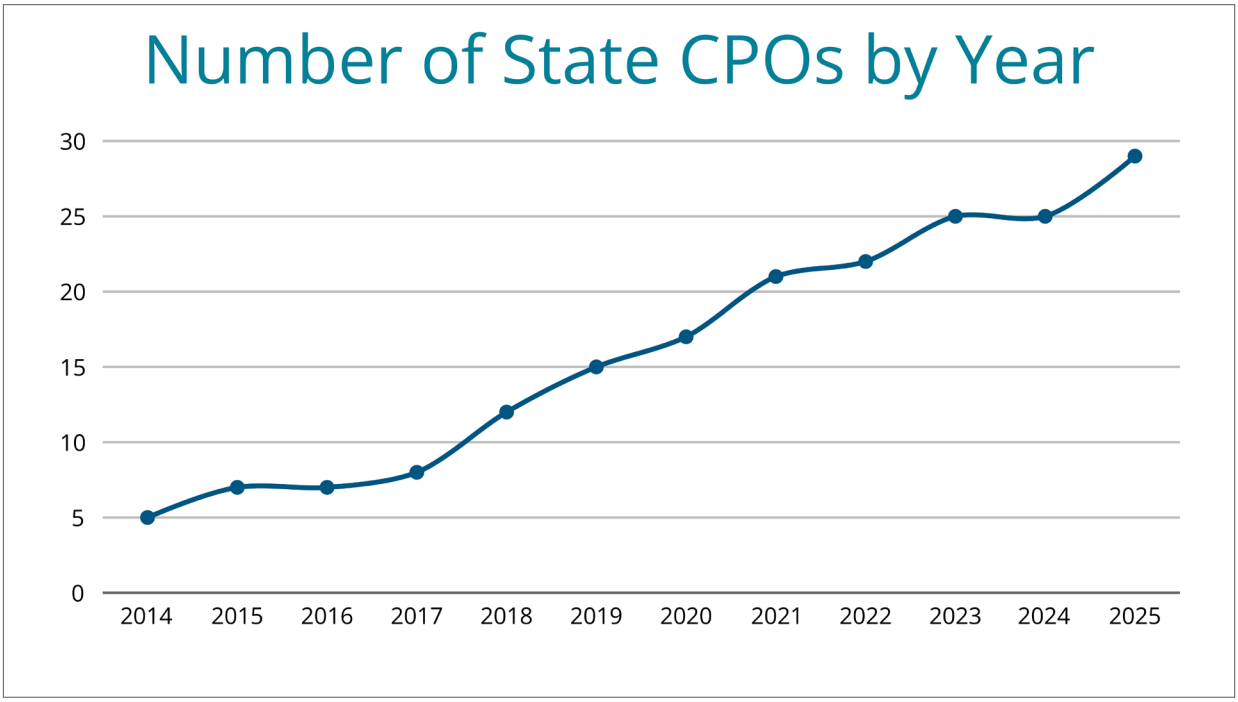


NASCIO®
Representing Chief Information Officers of the States

Creating a Privacy Program:
A Roadmap for States

The role of the state chief privacy officer (CPO) is one of the fastest growing leadership roles in state government. In the ten years that NASCIO has been tracking the number of states with a chief privacy officer, that number has grown from five at the beginning of 2015 to around 30 today. While most of those 30 individuals have a chief privacy officer title, some of them have other titles or wear dual hats (for example they may also be a general counsel). We know from our last survey of state CPOs that around 25 percent report to the state chief information officer (CIO) and around 20 percent report to the state chief information security officer (CISO).

There are several factors influencing the growth of privacy in states. In the absence of federal privacy legislation, states are enacting their own privacy laws, leading to greater awareness of privacy issues. Data breach notifications arrive in our inboxes more regularly, and citizens are becoming more aware of privacy rights. As the state CIO operating model evolves to include more private-sector partners handling citizen data, states are aware of the need for sound privacy practices in the acquisition process. Finally, as states embrace digital government services and the use of artificial intelligence, more data is being collected and processed than ever before.



One of the many tasks given to a new state CPO is to create a privacy program for the state or their agency. This can feel overwhelming on top of the daily deluge of tasks facing a state CPO or privacy manager. If an individual is new to creating a privacy program, the Certified Information Privacy Manager certification from the IAPP is valuable either as a first step or as something to work on alongside developing the privacy program.

Even if the federal government were to pass a comprehensive privacy bill, it would likely focus on consumer privacy, leaving states to establish or continue to implement their own privacy governance frameworks, define obligations and manage oversight and enforcement for state entities. This report includes a basic roadmap for states and state CPOs to create a privacy program.

State IT operating models are trending toward more consolidation and centralization. A CPO in a more centralized IT operating model (or other similarly centralized agency) that has authority over the executive branch agencies may be able to execute this roadmap themselves. In a more federated operating model state, where the CPO only has authority over their own agency or a limited number of agencies, they can serve as a resource to other agencies to follow these steps within their own organization.

Phase 1: Establish Foundations

1. Define Vision and Mission: Craft a privacy vision and mission aligned with the agency or state goals. This statement should set the tone for the privacy program and communicate its importance to all stakeholders. The mission statement should be two or three short sentences and take less than 30 seconds to read.

Below is an example of a privacy mission statement from Texas:

"[State] prioritizes safeguarding personal privacy. Responsibly handling our residents' personal information establishes trust in state government. As an employer, a collector of data from millions of individuals, and an advisor of information-management standards and policy, [Agency] strives to establish strong privacy policy, implement best privacy practices, and provide resources for our state agencies to do the same."

2. Gain Leadership Support: Secure executive buy-in and designate a privacy sponsor to champion the program. If no CPO has been identified or hired, find someone in the organization who is willing to take on privacy (this could be a deputy general counsel or program manager to start with). Emphasize the importance of privacy for trust, compliance and organizational reputation. The state CIO and/or the state CISO are uniquely positioned to be champions for privacy.

3. Assess Regulatory Scope: Determine the authority and scope of the program. Is the program intended as an educational resource for state agencies or does it have broader authority to require agencies to conduct assessments, implement policies and conduct training? Can the CPO enforce compliance with policies and laws? Alongside the program scope, identify applicable privacy laws and regulations (state, federal or international). Understand which laws affect your state operations and ensure they are included in your scope. Distinguish between privacy practices that are legally required and those that are optional under a framework. While recent comprehensive state privacy laws generally apply only to the private sector, some states have separate privacy laws governing the public sector.

Phase 2: Develop Governance

4. The Data Lifecycle: Map the data lifecycle. Identify what personal data is collected, how it's processed, stored and shared. Include physical and digital data. In states with a federated IT model, each agency may manage its own data. In those states, the CPO can offer guidance and resources for how to identify and map the data lifecycle.

5. Select a Framework: Adopt a recognized privacy framework such as NIST Privacy Framework, GDPR principles or ISO/IEC 27701. These provide templates for compliance and operational consistency. Many privacy laws start with the Fair Information Practice Principles as their foundation. Some states have incorporated a privacy framework into an already existing cybersecurity framework. Here is an example of a privacy framework from Washington Technology Solutions.

6. Structure a Team: While it's not always possible to hire staff in the first years of building a program, the goal should be to build a privacy team, assigning clear roles and responsibilities. In addition to having a team dedicated to privacy, develop a network of privacy contacts in the agencies and establish opportunities for the privacy network to communicate regularly. The structure of the "privacy team" may depend on the governance model of the state (centralized, federated or hybrid).

Phase 3: Operationalize Privacy

7. Conduct a Data Inventory: Create a record of processing activities (ROPA) and assist agencies in doing the same for the data they maintain. Use tools or surveys to document where personal data resides and how it flows across systems.

8. Develop Policies and Procedures: Write clear, enforceable policies covering data use, retention, breach response and employee privacy practices. Customize policies to meet both regulatory and organizational needs. Identify privacy duties that apply to all state agencies (possibly including records management, retention and data protection requirements) to ensure consistency and compliance across agencies. Develop a relationship with the state CISO and discuss where privacy and security policies overlap and coordinate.

9. Implement Privacy by Design: Ensure that privacy considerations are embedded into processes, services and technologies from the outset, not as afterthoughts. Managed services, software-as-a-service, cloud services, off-premise solutions and generative AI all have privacy implications. Implement a privacy impact assessment process to evaluate and document privacy risks before new a new technology or service is procured or developed.

Phase 4: Build Awareness

10. Launch Training Programs: Educate employees on privacy obligations, secure handling of personal data and incident response and tailor training to different roles and responsibilities. Some states have been successful in adding privacy training to regular cybersecurity training. Some states have also coordinated CIPM training for agency privacy officers through the IAPP so that each agency has a trained and certified privacy representative.

11. Engage Stakeholders: Establish a privacy council with representatives from HR, IT, legal, security, records management, data management and other key departments. Regularly communicate program updates and collaborate on solutions. This council ensures that the privacy program is aligned with cybersecurity, data management and records management policies and procedures.

Phase 5: Incident Management

12. Develop a Breach Response Plan: Create a detailed incident response plan. This will likely be a close collaboration with the state CISO. Clarify roles, reporting timelines and communication strategies. Conduct tabletop exercises to test readiness.

As an example, see the Texas DIR Incident Response Team Redbook Template.

13. Communicate with Regulators and the Public: Have a clear plan for meeting reporting obligations and managing public relations during a breach. This plan could be included in the incident response plan or could be a separate data breach notification plan.

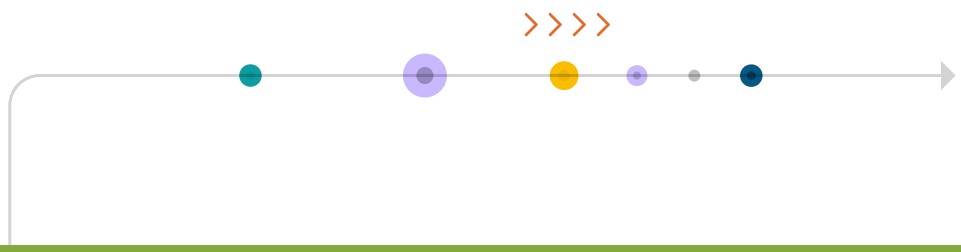
Phase 6: Monitor and Improve

14. Create Metrics and Monitoring: Track key performance indicators (e.g., data breach incidents and incident response times, training completion rates). Use metrics to demonstrate program effectiveness and identify areas for improvement.

15. Audit and Adjust: Regularly conduct both internal and external audits of the privacy program to ensure compliance and operational efficiency. Keep abreast of changing privacy laws, regulations and best practices by participating in regular privacy training events and conferences. Adapt to new laws, technologies and organizational changes.

Final Thoughts

Starting a privacy program from scratch can feel overwhelming, but focusing on key priorities like legal compliance and data inventory—while also building a privacy-first culture—will set you up for success. It won't be perfect right away, and that's okay. By regularly refining your approach as your program grows, you'll stay aligned with the evolving privacy goals of your state or organization.



Primary Author

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

Contributors

Christopher Bramwell, CIPM
Chief Privacy Officer
State of Utah

Jennie Hoelscher, CIPP/US
Privacy Officer & Assistant General Counsel
Office of General Counsel,
Texas Department of Information Resources

Katy Ruckle, CIPP/US, CIPM, FIP
State Chief Privacy Officer
Office of Privacy and Data Protection,
Washington Technology Solutions

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.