



# Observations on the State and Local Cybersecurity Grant Program (SLCGP)

NSCL Task Force on Artificial Intelligence, Cybersecurity and Privacy  
August 4, 2024

Doug Robinson, Executive Director  
@NASCIO

# 2024 FEDERAL ADVOCACY PRIORITIES



**Ensure Responsible Implementation of the State and Local Cybersecurity Grant Program**



**Expanding and Strengthening the State Cyber Workforce**



**Harmonize Disparate Federal Cybersecurity Regulations**



**Continued Adoption of DotGov Domain is Essential**



**Artificial Intelligence: States Leading the Way**

# 2024 STATE CIO TOP 10 PRIORITIES

Priority Strategies, Management Processes and Solutions

**1** CYBERSECURITY AND RISK MANAGEMENT 


**3** ARTIFICIAL INTELLIGENCE / MACHINE LEARNING / ROBOTIC PROCESS AUTOMATION 

**5** WORKFORCE 

**7** BROADBAND / WIRELESS CONNECTIVITY 

**9** CLOUD SERVICES 

**1** DIGITAL GOVERNMENT / DIGITAL SERVICES 

**4** LEGACY MODERNIZATION 

**6** DATA MANAGEMENT / DATA ANALYTICS 

**8** IDENTITY AND ACCESS MANAGEMENT 

**10** CIO AS BROKER / NEW OPERATING MODEL 

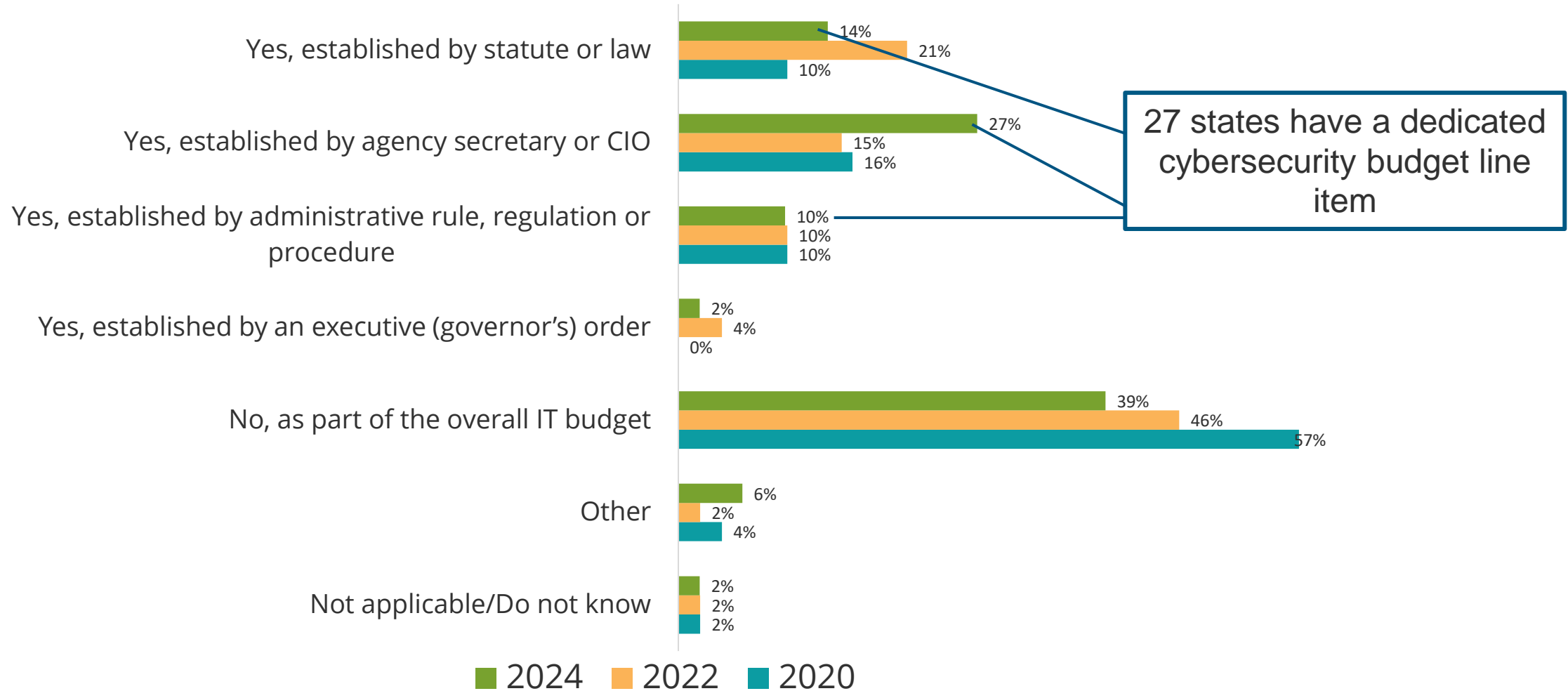


# Identify your state's top five (5) cybersecurity initiatives for 2024-2025

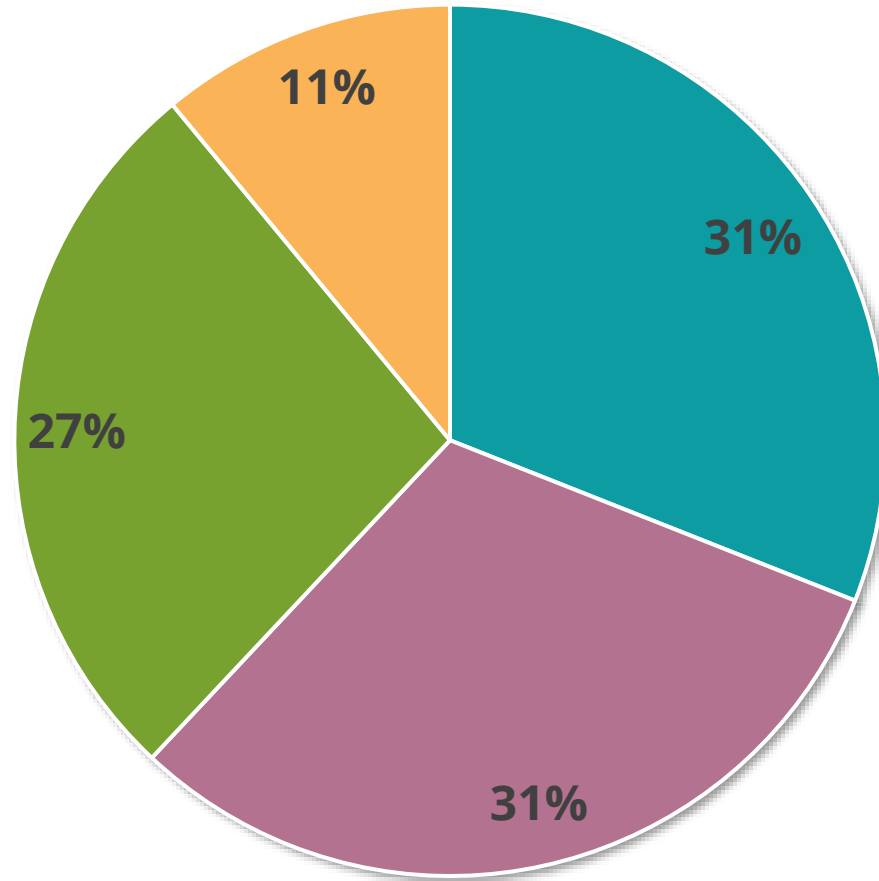
Rank	Option
1	Align cybersecurity initiatives with those of the business
2	Enterprise identity and access management
3	Risk assessments
4	Cloud platforms and solutions security
5	Extending state's enterprise security office to support local governments and public education
6	Governance (e.g., roles, reporting structures and directives)
7	Monitoring/security operations center
8	Implementing GenAI security controls
9	Metrics to measure and report effectiveness
10	Citizen digital identity



# Does your state have a cybersecurity budget line item?



# For the current program year of the SLCGP, how is your state administering the funds?



- 100% direct / pass through funds to local governments
- 100% shared cybersecurity services offered to local governments
- Hybrid of direct funding and shared services
- Other



# Under the SLCGP, which shared services is your state offering local governments?

Shared Service	Percent
Cybersecurity training	77.4%
Endpoint detection	51.6%
Risk assessments	45.2%
Support for .gov domain adoption	35.5%
Security monitoring	29.0%
Tabletop exercises	29.0%
Vulnerability management	29.0%
Incident response	25.8%
Statewide security operations center	25.8%
Governance and oversight	22.6%
Identity and access management / multi-factor authentication	19.4%

“Our statewide program has been widely embraced and we have provided training and end point protection to over 20,000 people in local roles (city and county).”



# Would you support a federal cybersecurity grant program that is targeted only to state government?

- Almost “Yes” from all, but almost all ALSO said that such a program shouldn’t undermine whole-of-state or siphon support from local governments
- One CIO said that the greatest concern in the state is “for our municipalities - we need to account for their concerns and help build them up to be prepared.”
- Another expressed that while a state specific program “would be very valuable, it is essential to support all local forms of government as well.”
- Multiple respondents also stated that while grant programs are helpful, long-term, dedicated funds that do not require increasing matches from the state are a more comprehensive and effective solution than the current SLCGP model.





# Are you satisfied with the grant funds available through the state and local cybersecurity grant program?

- The funding amounts in consideration of the mission and primary focus of SLCGP will not result in significant improvements in strengthening cybersecurity practices and resilience of the SLT governments.
- This level of funding is not enough to make a dent on the needs across the state. It is off by an order of magnitude at least if you include critical infrastructure such as drinking water and wastewater.
- The grant funding amount available is not enough to even scratch the surface for the cybersecurity needs at the local level.
- Grant funds are an important initial boost for many under funded organizations for cybersecurity improvements. However, governance & structure of the program needs better definition & more direct control by cybersecurity experts in the state.
- It is not enough to make a material improvement of the cyber risk posture across the entire local government sector.
- More funds should be appropriated over time to satisfy continuing obligations municipalities will face
- More funding is necessary to significantly move the needle for LGEs
- More funding is needed to support the State portion to support Local government
- The program was oversold to the local governments. The match requirement is a burden.
- Grant funds are insufficient to meet needs.
- To many regulations and red tape



# Summary Observations on SLCGP

- While all states have embraced a whole of state approach to cybersecurity to some degree, the flexibility to tailor SLCGP plans to the needs and goals of each state has been a key to its success so far.
- Almost 100% of respondents said SLCGP should be extended beyond 2026

