Generative AI in the States: Priorities, Trends and Recommendations

NSCL Task Force on Artificial Intelligence, Cybersecurity and Privacy

February 8, 2025

Doug Robinson, Executive Director
@NASCIO

2025 STATE CIO TOP 10 PRIORITIES

Priority Strategies, Management Processes and Solutions

1 CYBERSECURITY AND RISK MANAGEMENT

2 ARTIFICIAL INTELLIGENCE / MACHINE LEARNING / ROBOTIC PROCESS AUTOMATION

3 DIGITAL GOVERNMENT / DIGITAL SERVICES

4 DATA MANAGEMENT AND ANALYTICS

5 LEGACY MODERNIZATION

6 BUDGET / COST CONTROL / FISCAL MANAGEMENT

7 IDENTITY AND ACCESS MANAGEMENT

8 CLOUD SERVICES

9 WORKFORCE

10 ACCESSIBILITY

NASCIO Considerations for Developing AI Roadmaps

1. Align AI initiatives to strategic drivers for the organization

2. Establish governance and oversight processes

3. Inventory and document existing AI applications

4. Address data quality and sourcing

5. Collaborate with stakeholders and industry

6. Assess privacy and cybersecurity risks of AI adoption

7. Infrastructure and technology

8. Create acquisition and development guidelines

9. Identify potential use cases

10. Expand AI workforce expertise and training

11. Create guidelines for responsible use, ethics and transparency

12. Measure and communicate effectively

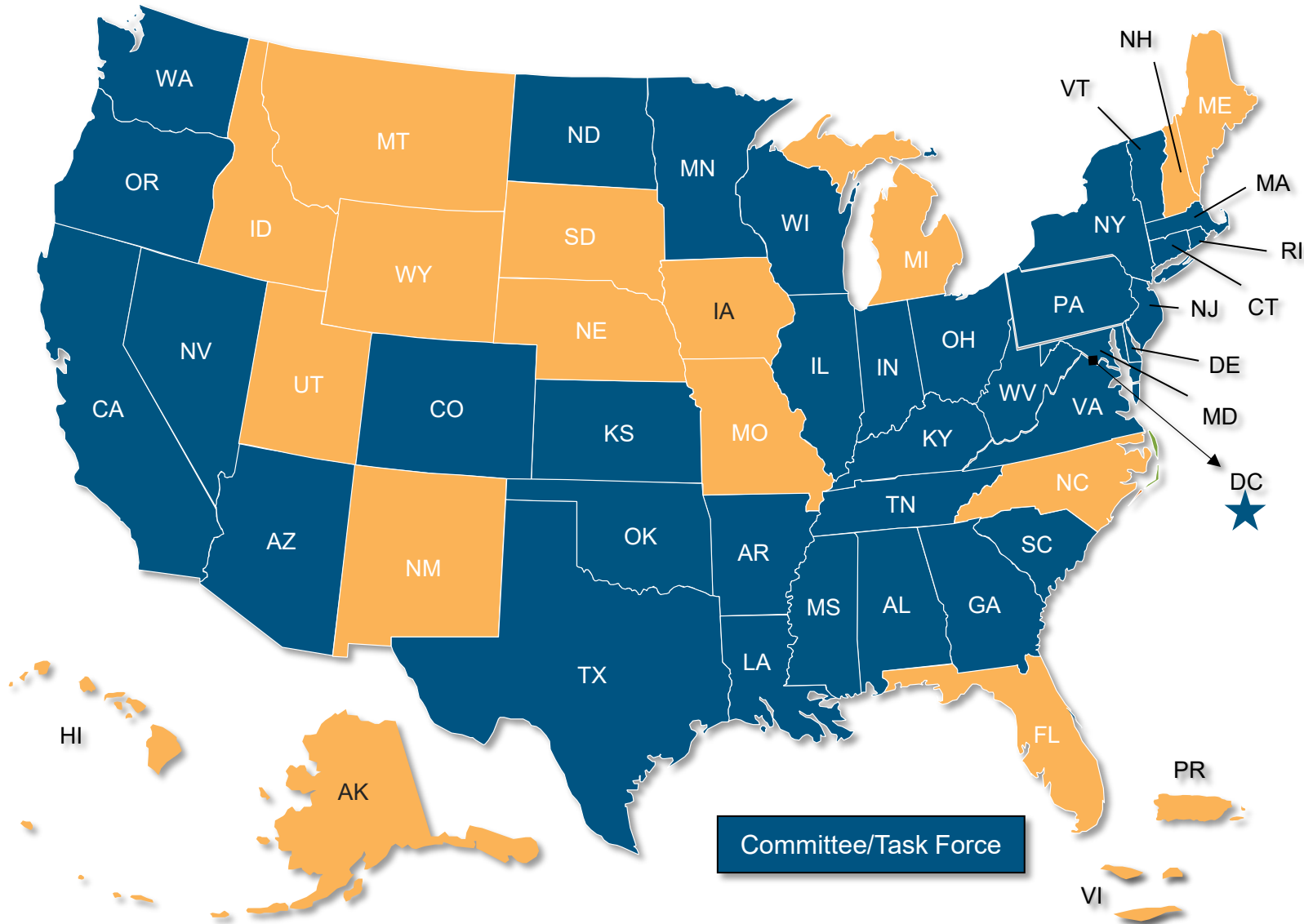NASCIO
Representing Chief Information Officers of the States

Top AI Actions Taken by States

▶ The creation of advisory committees and task forces (78%)

▶ Implementing enterprise policies and procedures on development/use (72%)

▶ Responsible use / flexible guardrails / security / ethics (67%)

▶ Inventory / documenting uses in agencies and applications (61%)

2024 State CIO Survey

State AI Committees and Task Forces
January 2025

Committee/Task Force

NASCIO
Representing Chief Information Officers of the States

Top Business Process Where States are Using GenAI

In Use

1 Virtual meeting assistant transcription

2 Cybersecurity operations

3 Document generation and management

4 Software code generation

Piloting

1 Document generation and management

2 Data analytics

3 Virtual meeting assistant transcription

4 Software code generation

Respondents allowed to make multiple selections

NASCIO
Representing Chief Information Officers of the States

State IT Use Cases for Generative AI

- Generating ideas, crafting emails, streamlining research
- Analyzing survey data and making recommendations
- Cataloging databases and identifying their owners
- Monitoring new legislation and creating a summary
- Coding assistance; legacy code interpretation and/or conversion
- Human resources: writing job descriptions
- Streamline procurement (repetitive forms, communication)

State IT Use Cases for Generative AI (cont.)

- AI-enabled bots to assist call center agents
- Cybersecurity threat detection, identify anomalies
- Language translation for online services
- Analyzing vehicle crash data
- Streamline health care facility inspections
- Supporting virtual agent chatbots to help citizens
- Fraud prevention and detection
- Improve traffic patterns and reduce congestion

Challenges for States: GenAI Adoption

- **Poor data quality/integrity**
- **Lack of enterprise governance**
- **Workforce skills gap / lack of training**
- Shadow GenAI use by employees
- Long-term costs
- Legal issues; public records creation
- Accessibility – design and interface
- Technical infrastructure
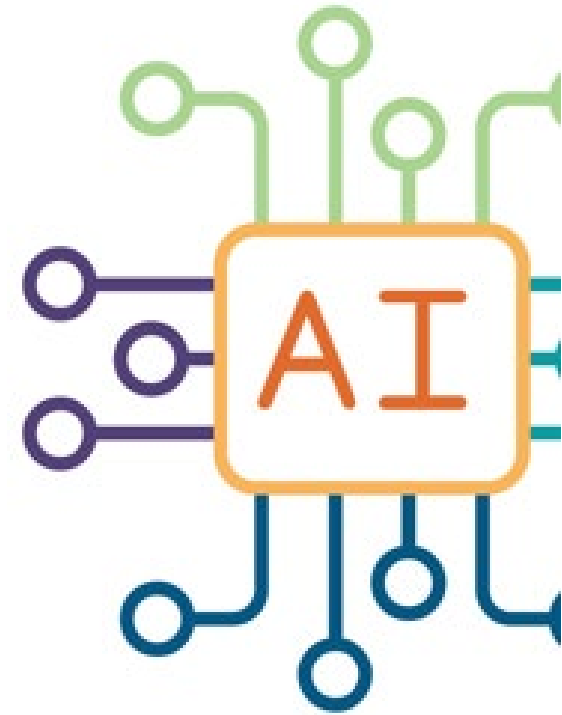
Generating Opportunity:

The Risks and Rewards of Generative AI in State Government

November 2024

NASCIO
Representing Chief Information Officers of the States

"Our potential use cases span from human resources, correspondence, policy development, review and access, GIS modeling, data analytics, customer engagement, accelerating legacy code review for modernization efforts, coding, security, contracts and procurement process improvement efforts."

"GenAI can document large scales of what this code is meant to do, give recommendations on how to break it up or modernize it, and then recode it,"

"Generative AI sometimes will give incorrect answers, or partially correct ones. So, with AI-assisted solutions, our government services have to be very carefully crafted and tested to minimize this."

"There won't be less jobs, but there will be different jobs. We have to make sure that the workforce is ready for an AI economy (or what's to come) and we must learn how to build an adaptive workforce."

"We have to consider the public perception, while it may not always be fair or accurate, artificial intelligence requires us to go carefully and be transparent in everything we are doing. We must over share, be thoughtful and have a steady approach."
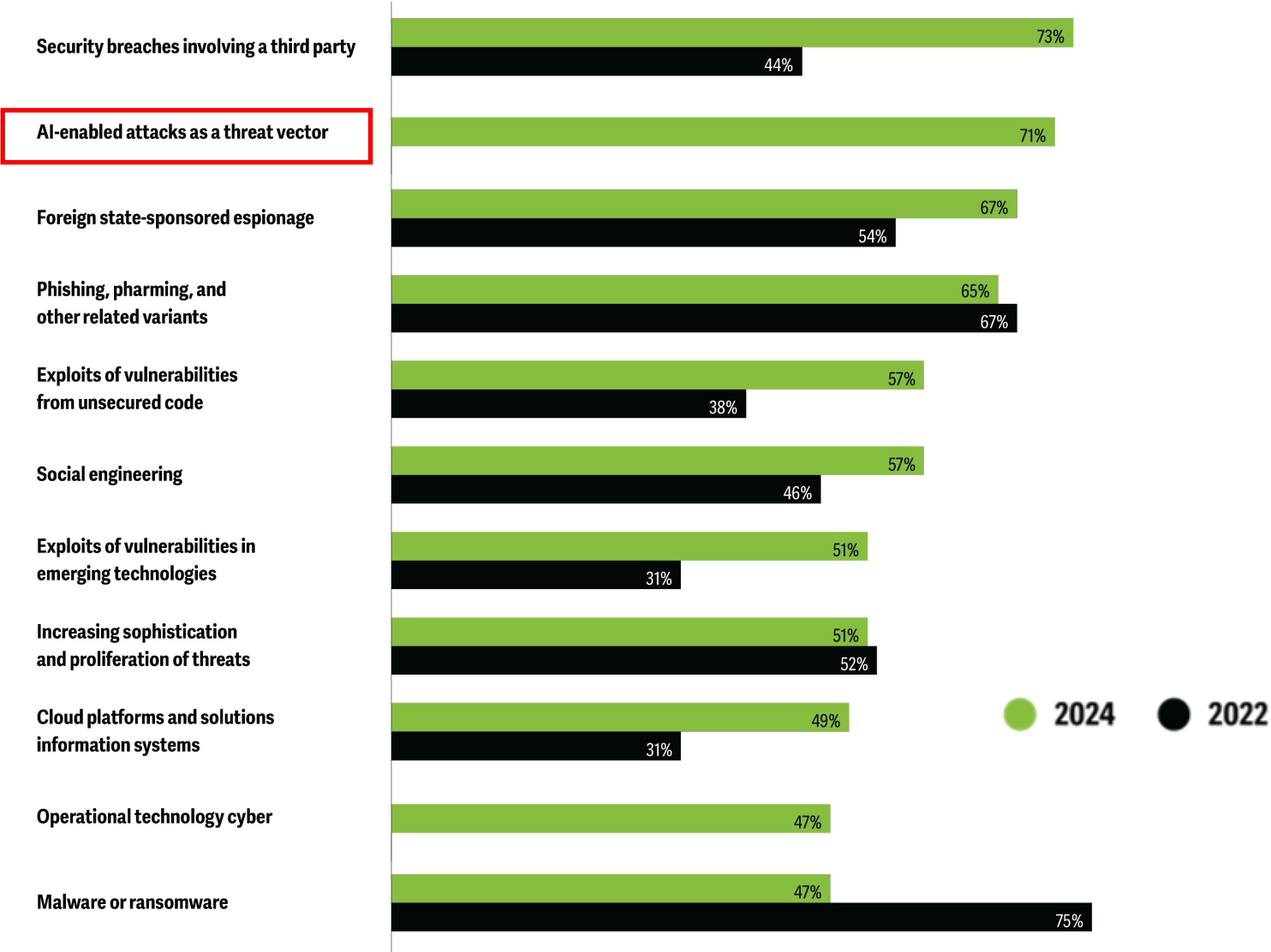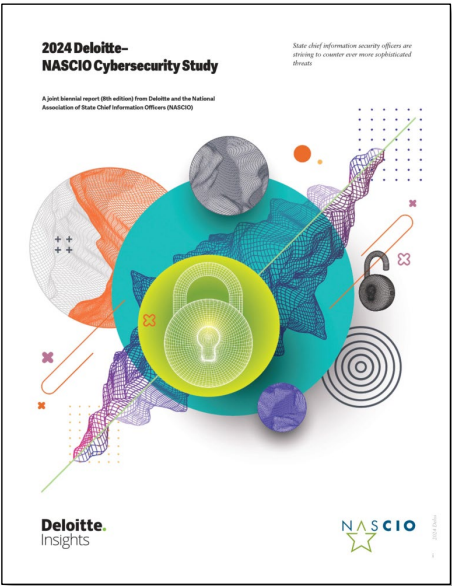
"We want GenAI to get to the point where we don't have unintended consequences."

Recommendations for States Using Generative AI

1. **Encourage Exploration and Set Policies.** Promote a culture of exploration and learning with generative AI. Employees are likely already experimenting with these tools, so state CIO organizations should lead the way by setting clear policies and guidelines for their use.

2. **Establish Strong Governance and Regulatory Frameworks.** Ensure that a robust regulatory and governance framework is in place before widespread AI adoption. This includes setting up guardrails to protect privacy and ensure responsible use, as well as creating a risk-based maturity scale to manage AI deployment from low to high risk.

3. **Focus on Data Quality.** The effectiveness of AI systems is heavily dependent on the quality and accessibility of data. Prioritize data governance, including data retention policies, and work closely with state CDOs to ensure clean and reliable data.

4. **Build Partnerships and Foster Collaboration.** Develop strong partnerships with peers across different departments and agencies.

5. **Adopt an Incremental Approach.** Start with small, low-risk pilot projects to identify potential use cases and build on lessons learned.

6. **Be Transparent.** Communicate openly about AI initiatives, including successes and limitations. Transparency with constituents about data practices and AI usage is crucial for building trust.
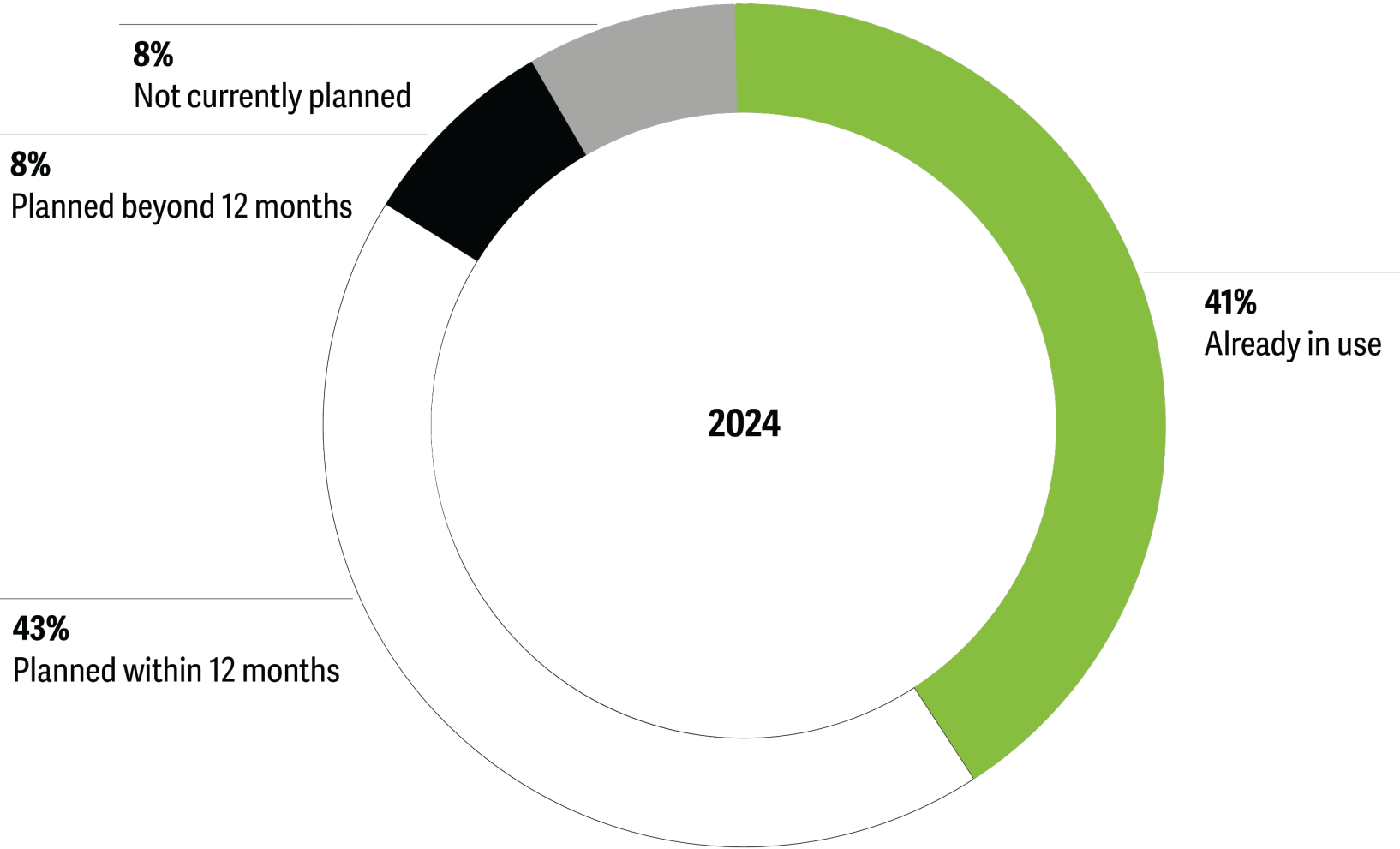
Leading causes of a cybersecurity incident in states over the last year

2024 Deloitte–NASCIO Cybersecurity Study

State chief information security officers are striving to counter ever more sophisticated threats

A joint biennial report (8th edition) from Deloitte and the National Association of State Chief Information Officers (NASCIO)

Deloitte. Insights

NASCIO

Cause	2024	2022
Security breaches involving a third party	73%	44%
AI-enabled attacks as a threat vector	71%	
Foreign state-sponsored espionage	67%	54%
Phishing, pharming, and other related variants	65%	67%
Exploits of vulnerabilities from unsecured code	57%	38%
Social engineering	57%	46%
Exploits of vulnerabilities in emerging technologies	51%	31%
Increasing sophistication and proliferation of threats	51%	52%
Cloud platforms and solutions information systems	49%	31%
Operational technology cyber	47%	
Malware or ransomware	47%	75%

● 2024   ● 2022

Note: The 2022 survey did not include the options "AI-enabled attacks as a threat vector" and "operational technology cyber.".

NASCIO

Representing Chief Information Officers of the States

2024 Deloitte-NASCIO Cybersecurity Study

Current and planned use of GenAI in state cybersecurity operations

- 8% Not currently planned
- 8% Planned beyond 12 months
- 41% Already in use
- 43% Planned within 12 months

2024

2025 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

NAS CIO
Representing Chief Information Officers of the States