NASCIO
Representing Chief Information Officers of the States

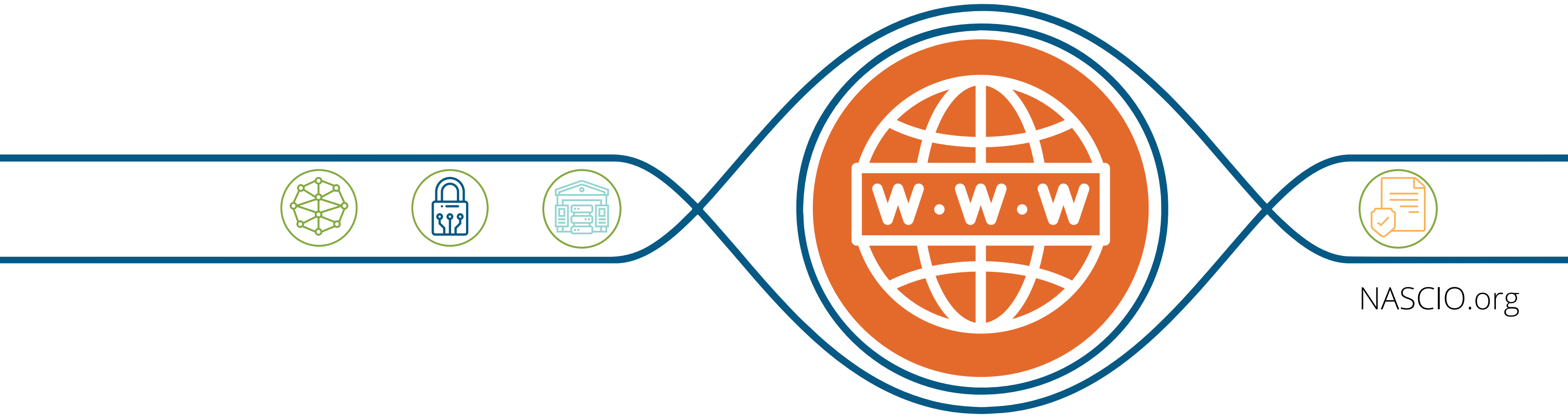
Widespread Adoption of DotGov Domain is Essential

Issue and Background

- The DotGov domain provides enhanced security features and increases the public trust in government.
- With rampant misinformation and disinformation campaigns from issues ranging from election security to COVID-19, it is paramount that citizens receive accurate and trusted information from government websites.
- Nearly twenty years after making DotGov available to state and local governments, only approximately 8.5 percent of local governments are registered on the domain.
- With the vast majority of local government websites on domains other than DotGov, there is no official governing body validating whether their websites are legitimate entities or fraudulent actors.
- In the 116th Congress, NASCIO endorsed the DOTGOV Act, introduced Senators Gary Peters (D-MI), Ron Johnson (R-WI), Amy Klobuchar (D-MN) and James Lankford (R-OK), which was passed and signed into law in December 2020.
- Under the new law, DOTGOV program will be managed by DHS CISA and require them to develop an outreach strategy to inform and support the migration to the DotGov domain of local governments. DHS CISA will provide technical information on how to migrate online services to DotGov. The law also allows State Homeland Security Grant Program funds as an allowable expense for the adoption of the DotGov domain and further stipulates that the CISA Director may waive any fees associated with DotGov registration.

Recommendation

- **The DotGov Program should be free to all eligible entities**. One significant barrier of adoption is the $400 annual registration fee, which many local governments identify as being cost prohibitive. CISA should work to remove all associated fees to further incentivize adoption.
- **Provide flexible usage of State Homeland Security Grant Program funds** to be used for migration to DotGov domain to include non-technical transition costs on items including stationary, business cards and marketing materials.
- **CISA should establish a stakeholder advisory group** to include State CIOs and CISOs to provide feedback and input on their outreach strategy to local governments, work with local governments to highlight the security enhancements of DotGov, as well as to assist in migration to DotGov domain.



NASCIO

Representing Chief Information
Officers of the States

Expand Broadband Access and Affordability

Issue and Background

- As the ongoing COVID-19 pandemic quickly forced the vast majority of America's workforce into a remote and virtual setting, the importance of reliable and affordable broadband has never been more of a paramount issue facing our nation.
- While broadband expansion, and expansion of networks to rural areas of the country, has been a significant priority at the federal and local level, there are still nearly 18.5 million Americans who lack even basic access to broadband, according to the National Governors Association (NGA).
- State CIOs understand the importance of broadband in supporting nearly every initiative in their portfolio – from improving digital government services to supporting remote work solutions to providing education and healthcare opportunities for their citizens.
- In this year's State CIO Survey, more than 80 percent of state CIOs contend that their state will now accelerate the implementation of their broadband strategies.
- Currently, the Federal Communications Commission (FCC) collects and maps all data on current broadband availability and service speeds. Some states have developed their own mapping capabilities that provide significantly more data at higher granularity as opposed to the FCC's model of capturing data at a census-block level.
- Inaccurate and outdated broadband coverage maps create a significant issue that needs to be addressed to improve connectivity across the country. This mapping methodology is also currently tied to funding for broadband deployment.

Recommendation

- **Streamline existing federal funding.** Congress should look to streamline existing federal funding for broadband as current sources of funding have proven difficult to navigate for most states. Current funding sources are also primarily tied to specific programs, which constrain state and local governments from best utilizing funds.
- **Increase partnerships between state and federal governments.** Congress and the FCC should increase and enhance these partnerships to resolve the numerous challenges associated with broadband expansion in rural and low-income areas across the country. These challenges include lack of economic incentive for internet providers and lack of competition that keep broadband prices too high.
- **Leverage state-led broadband mapping strategies.** Congress and the FCC should look to leverage broadband mapping strategies that have been deployed in state broadband offices, including Georgia's Broadband Deployment Initiative, to challenge and amend the FCC's broadband data collection processes. A more accurate mapping process will result in improved tools to inform citizens and measure the progress of broadband programs.

Authorize and Appropriate a Dedicated Cybersecurity Grant Program for State and Local Governments

Issue and Background

- There is a growing recognition at all levels of government that cybersecurity is no longer an IT issue; it is a business risk that impacts the daily functioning of our society and economy, as well as a potential threat to our nation's security.
- State CIOs continue to face an increasingly complex cybersecurity threat environment without dedicated cybersecurity funding.
- Cybersecurity has remained the top priority for the State CIOs for the past eight years, according to the 2020 NASCIO State CIO Survey.
- Only half of all states have a dedicated cybersecurity budget line item while federal government agencies and private sectors allocate a significant percentage of their IT budget on cybersecurity.
- According to the 2020 Deloitte-NASCIO Cybersecurity Study, state cybersecurity budgets are less than three percent of their overall IT budget and face further cuts due to the bleak economic outlook as a result of the COVID-19 pandemic.
- State and local governments remain, and will remain, attractive targets for cyber-attacks as evidenced by dozens of high-profile and debilitating ransomware incidents with a financial cost of more than $7.5 billion in 2019, according to EMSISOFT.
- Current federal funding for state and local government cybersecurity has proven inadequate with less than four percent of all State Homeland Security Grant Program funding allocated to cybersecurity over the last decades.

Recommendation

- **Authorize and appropriate a federally funded cybersecurity grant program** that would allow state CIOs to better assist local government partners and thwart well-funded nation-states and criminal actors that continue to grow in sophistication.
- **In the 116th Congress, NASCIO endorsed numerous bipartisan and bicameral bills that would create new grant programs for state and local governments to bolster their cybersecurity posture**. These bills include: S. 1846, the *State and Local Government Cybersecurity Act*, H.R. 5823, the *State and Local Cybersecurity Improvement Act*, S. 1065/H.R. 2130, the *State Cyber Resiliency Act* and H.R. 8048, the *State and Local IT Modernization and Cybersecurity Act.* These bills should serve as a model for legislation in the 117th Congress.

NASCIO

Representing Chief Information
Officers of the States

Provide Funding for State Governments to Modernize Legacy IT Systems

Issue and Background

- States are the primary agents for the federal government to deliver vital services to citizens across the country. The ability to safely and securely deliver these services has taken on unprecedented importance during the ongoing pandemic.
- As the highest-ranking technology officials in their state, CIOs are tasked with implementing information technology (IT) policies and business practices to ensure the timely and secure delivery of essential services to citizens.
- These federal services and programs include Medicaid, food and nutrition assistance, unemployment insurance and critical justice information.
- Most of these programs operate on outdated and legacy technology systems that are susceptible to failure and cyber-attacks, including sophisticated ransomware attacks.
- The COVID-19 pandemic has unfortunately revealed – with real-world consequences – how many states and localities have struggled to deliver essential services, from unemployment benefits to public health tracking data, due to outdated IT infrastructure.
- IT modernization requires a significant level of flexible, agile funding to effectively plan for and finance multi-year modernization efforts. In the 116th Congress, NASCIO advocated for the inclusion of IT modernization funding for state and local governments in COVID-19 stimulus legislation.
- In the 116th Congress, NASCIO endorsed the *State and Local IT Modernization and Cybersecurity Act*, introduced by Reps. James Langevin (D-RI) and Mike Gallagher (R-WI), which would establish a Public Health Emergency Information Technology Grant Program and a Modernizing Information Technology Program for state and local governments.
- The legislation would allow for the migration of legacy systems to new, secure platforms in line with and state IT modernization strategies reviewed by the Cybersecurity and Infrastructure Security Agency (CISA).

Recommendation

- **NASCIO urges Congress to fund a grant program to allow state and local governments to migrate legacy IT infrastructure to modern, secure platforms**.
- **The *State and Local IT Modernization and Cybersecurity Act* should serve as a commonsense and bipartisan example** of a grant program that would immensely improve the IT infrastructure for state and local governments. IT modernization is vital not only because it saves money and enhances cybersecurity, but it is the primary means for states to deliver vital services securely and capably to the American people.

Harmonize Disparate Federal Cybersecurity Regulations

Issue and Background

- As the primary agent of the federal government, states administer dozens of crucial federal programs and deliver vital services to citizens. As a result, state governments must store data and exchange data with federal programmatic agencies and thus become subject to federal security regulations that govern the use and protection of shared data.
- Federal cybersecurity regulations largely address the same controls and outcomes but differ in their specific requirements.
- Compliance with disparate regulations is an obstacle for state CIOs who are actively seeking savings for taxpayers through IT initiatives like consolidation/optimization. Further, when state data centers are audited for compliance, states receive inconsistent findings from federal auditors despite reviewing the same IT environment.
- As state IT agencies have become increasingly centralized across the country – whereby the state CIO has greater purview over the IT operations of each state agency – compliance with duplicative requirements of federal cybersecurity regulations has grown significantly in cost, both financial and in personnel time.
- In 2018, Congress tasked the Government Accountability Office (GAO) to study the various federal cybersecurity regulations and to issue corresponding recommendations.
- In May 2020, GAO issued their report, *Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, which found that between 49 and 79 percent of federal agency cybersecurity requirements had conflicting parameters and urged the federal agencies to collaborate on cybersecurity requirements.

Recommendation

- **Congress and the federal agencies should implement the recommendations of the GAO report and requests the Office of Management and Budget (OMB) to coordinate collaboration among federal agencies on the development and implementation of cybersecurity regulations.**
- **Federal agencies should work with State CIOs and CISOs to streamline cybersecurity regulations.** Addressing duplicative regulations and inconsistent audit practices will not only save taxpayer funds but will also improve our nation's cybersecurity posture. State CIOs remain committed to working with federal agencies and auditors to harmonize disparate interpretations of security regulations and to normalize the audit process.