NASCIO®
Representing Chief Information
Officers of the States

# Expand Broadband Deployment and Reform FCC Mapping Methodology

## 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.

- COVID-relief legislation (CARES Act and the American Rescue Plan Act) and the Infrastructure Investment and Jobs Act (IIJA) have provided unprecedented federal resources to improving broadband across the country.

- The IIJA includes $65 billion for broadband, including $42.45 billion in grants directly to the states. This represents the largest investment in broadband in American history. The IIJA also contains provisions requiring the FCC to reform their mapping methodology.

- 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, as well as participation in the 21st century economy.

- In this year's State CIO Top 10 Priorities, broadband was ranked by the state CIOs as their #3 priority, which includes strengthening statewide connectivity, implementing rural broadband expansion and 5G deployment.

- Currently, the Federal Communications Commission (FCC) collects and maps all data on current broadband availability and service speeds, which result in inaccurate and outdated broadband coverage maps. This creates a significant issue that needs to be addressed to improve connectivity across the country.

- In a November 2021 Congressional hearing, FCC Chairwoman Rosenworcel backed up this assertion by stating that her agency's maps simply "stink."

## Recommendation:

- **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.

- **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.

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

## 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.

- Cybersecurity has remained the top priority for the State CIOs for the past nine years, according to the 2022 NASCIO State CIO Top 10 Priorities.

- Less than 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.

- With the inclusion of the State and Local Cybersecurity Grant Program in the *Infrastructure Investment and Jobs Act*, states and localities have an unprecedented opportunity to improve their security posture, increase collaboration between state, local and federal governments and promote a whole-of-state approach to cybersecurity.

- The $1 billion/4-year program will be administered by FEMA with subject matter expertise from DHS CISA and requires significant input by state CIOs and CISOs, who are charged with approving and implementing a statewide cybersecurity plan.

## Recommendation:

- **Work with FEMA and CISA** to ensure grant guidance includes flexibility for states, promotes whole-of-state cybersecurity, emphasizes cyber hygiene, shared services models and establishes minimum requirements for local government eligibility to receive grant funding.

- **Continue to advocate for states to budget for cybersecurity.** The State and Local Cybersecurity Grant Program requires states to match a portion of federal funding, which increases by 10 percent each year. NASCIO contends this grant program should serve as a change agent for states to either begin to include cybersecurity in their state budget or increase their allocation. In line with Congressional intent and through federal assistance, state governments must realize cybersecurity cannot be solved with a one-time appropriation; inclusion of a cybersecurity line item is the minimum states should do to meet the seriousness and sophistication of the current threat environment.

- **Ensure state CIOs and CISOs set policy for the grant program**. While State CIOs and CISOs should not serve as grant administrators, they understand the unique cybersecurity challenges facing their state. In consultation with their planning committees, they should set policy parameters and prioritize funding opportunities for this grant program.

# 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.

- During a June 2021 hearing before the U.S. House Oversight Subcommittee on Government Operations, Chairman Connolly and Ranking Member Hice, as well as numerous other members of the Subcommittee, expressed frustration with the burdensome and duplicative regulations.

## Recommendation:

- **Congress and the federal agencies should implement the recommendations of the GAO report** and urge the Office of Management and Budget (OMB) to coordinate collaboration among federal agencies on the development and implementation of cybersecurity regulations.

- **Congress should empower OMB with requisite authorities** to ensure OMB can mandate consultation by federal agencies before updating their 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 and CISOs remain committed to working with federal agencies and auditors to harmonize disparate interpretations of security regulations and to normalize the audit process.

# Continued 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, less than 10 percent of local governments are registered on the domain.

- In April 2021, administration of the .gov top-level domain (TLD) was transferred from the General Services Administration to the Cybersecurity and Infrastructure Security Agency (CISA), reflecting the inherent linkage between domain registration and cybersecurity.

- NASCIO's advocacy was instrumental in CISA's announcement to waive the annual $400 registration fee for DotGov, which was cost prohibitive and unnecessarily burdensome for the majority of local governments.

- While waiving the registration fee was a key step in the right direction to increase migration to DotGov, there needs to be increased education, outreach and advocacy to local governments.

## Recommendation:

- **CISA should establish a stakeholder advisory group** to work with key stakeholders and educate local governments on the business case and security benefits of migrating to .gov. CISA should utilize the state CIOs and CISOs to assist in this educational campaign and to highlight a 24/7 help desk and other inherent operational benefits of the .gov program, which will provide tremendous support to resource and personnel-constrained local governments.

- **Expand opt-in centralized cybersecurity services for DotGov entities** CISA has built a strong team focused on providing technical support and information to SLTTs. With ownership of the .gov program, they can now make available opt-in cybersecurity shared services on top of the .gov TLD. Doing so will create a compelling case for local governments to migrate to a .gov and leverage the additional capabilities CISA can make available.

- **Tie federal grant funding for local governments to DotGov adoption/migration.** With the recent passage of the State and Local Cybersecurity Grant Program, local governments will receive 80 percent of federal funding. CISA and FEMA should mandate local governments will only be eligible for grant funding if they agree to migrate to the DotGov domain.

- **Allow 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 communication outreach to citizens, marketing materials and revisions to stationary, business cards and other printed collateral.