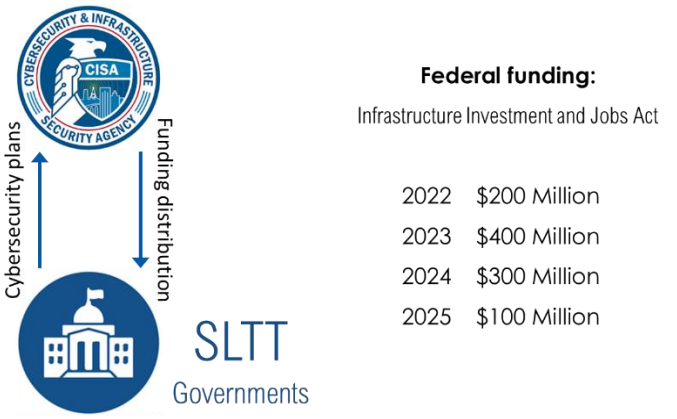
ATARC

# WHITE PAPER

## Federal Cybersecurity Funding to State and Local Governments

*Summary of Roundtable, hosted by ATARC on February 2, 2022*

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC), representatives from various Federal, State and Local organizations shared their thoughts on the expected distribution of $1 billion of federally approved cybersecurity funding included in the Infrastructure Investment and Jobs Act, also known as the Bipartisan Infrastructure Framework.




This approved funding is a culmination of years of advocacy from state and local governments, and the biggest government investment in state and local cybersecurity to date. Cybersecurity continues to be a critical issue for local governments. Cities all over the country experience cyber-attacks that cripple critical services and costs missions of dollars in recovery. Due to the lack of trained IT personnel, mature IT departments or security plans, localities are potentially more vulnerable to cybersecurity threats than Federal agencies that have more resources. As more services moved online during the COVID-19 pandemic, state and local governments have found themselves increasingly more vulnerable to attacks.

Cybersecurity funding available to state and local governments is set to be allocated over four years, with $200 million made available in 2022, $400 million in 2023, $300 million in 2024, and $100 million in 2025. Distributing these funds to state and local governments is now the primary challenge. In order to access this funding, state, local, territorial and tribal governments (SLTTs) will be required to present comprehensive cybersecurity plans through a grant program run by the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA).

ATARC's roundtable participants discussed the cybersecurity priorities and challenges facing local governments, how SLTTs can collaborate and partner to maximize benefits from the available funds, and considerations for localities when applying for funding. Roundtable participants also discussed ways the Federal government could potentially support localities in the application and implementation of cybersecurity funds.

## Local Priorities and Challenges

Cybersecurity initiatives have received significant attention and priority at the Federal level. Not only are Federal agencies more organized in their shared planning and


info@atarc.org

response to cybersecurity threats, there has been significant Federal cybersecurity policy driven by either presidential administrations or legislation through Congress. This collaborative and organized response to cybersecurity has resulted in well-equipped Federal agencies, making the government stronger from a cyber perspective.

In comparison, the ability to adequately address cybersecurity varies greatly among state and local agencies. The local cyber ecosystem is often comprised of different types of governmental entities, including school districts, municipalities, transportation authorities or counties. Localities, particularly those that are small or rural, are often challenged with a lack of resources to adequately address cybersecurity. These organization may not have properly trained personnel, available funding for security programs, or even a dedicated IT department. Other local organizations are quite mature, having prioritized cybersecurity and invested significant resources to secure assets and to develop a cybersecurity plan.

## Uniquely Local Challenges

- Varying functions of government entities
- Inadequate resources
- Lack of properly trained personnel
- Unique, niche cyber attack targets
- Specific attack patterns
- External dependencies for cybersecurity solutions

Cybersecurity issues at the state and local level are often characterized by unique, niche targets and specific attack patterns. The sophisticated and targeted nature of state and local cyber threats require state and local agencies to share intel, resources, talent and come together as a unified front to respond to attacks. Similar to mutual aid responses of public safety agencies, local organizations and municipalities should be utilizing this model when responding to cybersecurity threats.

## Mutual Support and Collaboration

Building strategic partnerships among local government entities through mutual support and aid can often harden cybersecurity threats. While there are challenges to full collaboration among various local organizations, including organizational cultures, structures and policies, any overlapping security measures can create a stronger response to threats if they were to occur. The ability to engage as a broader community with combined talents and tools can begin to address this ever-growing challenge on a local and regional level.
Smaller states share some of the unique challenges facing local governments. They may share infrastructure among one another, making collaboration and information sharing that much more critical. Townships in these smaller states will often have one or two IT employees, making it challenging for these localities to adequately plan and guard against cybersecurity threats. States are collaborating with smaller localities to ensure a united front against attacks by providing subscription-based services and Federal level guidance.

Roundtable participants concurred that in addition to mutual aid, a multidisciplinary approach is needed to address cybersecurity threats at the local level. Partnerships with other entities including universities may help to progress cybersecurity into other disciplines such as economic development and workforce recruitment and development.

## Funding Application Considerations

Roundtable participants discussed some of the criteria localities should consider when applying for the newly available cybersecurity infrastructure funding. As dictated by statute, the grant application evaluates 16 elements of a locality's IT capabilities. Because the maturity of local IT departments varies, some entities with few to no cybersecurity assets or those with external dependencies, may need to conduct a business impact analysis prior to applying in order to better articulate the needs of the organization.

Other entities with more mature programs may also benefit from conducting an assessment based on the National Initiative for Cybersecurity Education (NICE) framework. Roundtable participants suggested that localities should identify workforce gaps or skills training needed, and to include those figures in the grant application. Understanding what an organization currently has will help articulate what it needs.

Localities currently have access to CISA's Cyber Resilience Review, where CISA will help localities with cyber assessments. Having this baseline may also assist a locality's representation at the state and federal level and influence policy.

## Federal Support to Localities Applying for Cybersecurity Funds

When asked how the Federal government can support localities with cybersecurity efforts, roundtable participants provided a range of suggestions that include the Federal government providing clear application checklists, educational and training opportunities, and comprehensive guidance on cybersecurity best practices.

Participants noted that the application process should recognize and consider the cyber maturity and capabilities of local organizations. While some localities possess sophisticated cybersecurity playbooks, others do not have a threat management system at all. The latter will likely need hands-on guidance and support from the state or federal level in addition to funding. Because the needs of localities differ, it is important for the application to consider the customer in their unique stages of cybersecurity maturity, and whether the locality has ever responded to cyber threats or has concerns about a potential attack.

Participants recommend the Federal government develop online guidance and resources on the application and implementation of funds especially for localities. Localities could benefit from Federally suggested milestones, metrics, or periodic goals to better plan and prioritize the funding. In additional to online resources, participants suggested that a local CISA representative should be made available to localities for hands-on support and guidance.

## Suggestions for Federal Support

- Clear funding application checklists
- Educational and training opportunities
- Guidance on cybersecurity best practices
- Recognition of unique stages of cyber maturity and capabilities
- Considerations of specific concerns about a potential cyber threats
- Online guidance and resources
- Federally suggested milestones, metrics, and goals
- Local CISA representative for hands-on support

Panelists noted that small, rural communities make up the majority of most states, and are likely to rely on third party Managed Service Providers (MSPs) to carry out cybersecurity responsibilities. These external dependencies can become problematic when localities with few to no IT personnel rely on MSPs for their cyber protection.

Roundtable participants acknowledged the widening gap in cybersecurity skill in localities across the country, and stressed that the Federal government should provide training, skill development, and certification for local governments. Similarly, localities should also partner with higher education and wider education networks to address the widening talent gap.

Contact us today to learn more and get involved in the State and Local Cyber Grant Program Working Group!