State and Local Cybersecurity Grant Program:

- Included in the Infrastructure Investment and Jobs Act (IIJA)
- Authorizes the appropriation of $1 billion between 2022-2025 for the Department of Homeland Security to award grants to state, local and tribal governments to address cybersecurity threats and risks to their IT systems

OVERVIEW:

- $1 billion for the next four years starting in FY22:
  - FY22: $200 million
  - FY23: $400 million
  - FY24: $300 million
  - FY25: 100 million
- Within 45 days of receiving the grant, states and entities must make funding available to local governments.
- Eighty (80) percent of funding goes to local, tribal and territorial governments (25 percent to rural areas based on census data).
- State CIOs and CISOs serve as primary officials to manage and allocate funding.
- Five percent can be used for administrative costs, such as salaries and other related expenses.
- Plans must be approved by a planning committee and the state CIO/CISO (or equivalent official).
- The grant program permits multistate cooperative grant applications (two or more states apply for a grant jointly).

CYBERSECURITY PLAN:

The key item of the grant program and likely guidance for grant application focuses on the submission of a cybersecurity plan, which must be submitted to DHS CISA. A cybersecurity plan must include the following **required** elements:

- A description of any existing plans to protect against cybersecurity risks and threats to systems owned or operated on behalf of the state, local or tribal government with consultation from local governments and associations of local governments.
- An explanation of how the state will manage, monitor and track information systems, applications, and between information systems, including legacy IT systems.
- An overview of how the state plans to enhance preparation, response and resiliency of IT systems against risks & threats and utilize best practices, such as the NIST framework.
- How they plan to implement a process for continuous cyber vulnerability assessments and threat mitigation practices.

- How to ensure the adoption and use of NIST cybersecurity and supply chain security framework.
- How to promote the delivery of safe, recognizable, and trustworthy online services through the .gov domain.
- How to ensure continuity of operations in the event of a cyber incident, including promotion of cybersecurity exercises.
- How the state will enhance recruitment and retention of cyber workforce through the use of the NICE Workforce Framework.
- How the state will assess and mitigate cyber risks & threats related to critical infrastructure and key resources.
- How the state will communicate and coordinate with other states and DHS to address cyber risks & threats.
- A description and outline of the timetable and necessary resources for implementing the cybersecurity plan, including metrics the state will use to measure progress.

States **may** use the following discretionary elements in the submission of their cybersecurity plan:

- Consultation with MS-ISAC.
- Include a description of cooperative programs developed by groups of local governments to address cybersecurity risks and threats.
- Include a description of programs provided by the state to support local governments and owners and operators of critical infrastructure to address cybersecurity risks and threats.

PLANNING COMMITTEES:

States that receive grants shall establish a planning committee to:

1. Assist with the development and implementation of the cybersecurity plan
2. Approve of the cybersecurity plan
3. Assist with the determination of the effective funding priorities for the grant

Composition of Planning Committee: Representatives from the state, counties, cities, towns, institutions of public education and health within the jurisdiction, and tribes with members from suburban, rural and high-population jurisdictions with no less than half members having professional experience related to cybersecurity or IT.

Any existing planning committee or commission may be used if it meets the requirements and may be expanded or leveraged to meet the requirements.

FEDERAL-STATE MATCHING REQUIREMENT:

- The federal share of the cost of an activity carried out using the grant funds made available under the program may not exceed: 90% for FY22, 80% for FY23, 70% for FY24, 60% for FY25.
- The state share may not be an in-kind match. This will likely be needed via an appropriation by the state legislature.

GRANT FORMULA APPORTIONMENT:

- Baseline amount: .25% of such amounts to each of the territories; 1% of such amounts to each of the remaining states and 3% to tribal governments
- The remainder of such amounts will be apportioned by ratio:
    - 50%: Population of each state divided by the population of all states
    - 50%: Population of each state that resides in rural areas divided by the population of all states in rural areas

PROHIBITED USE OF GRANT FUNDS:

- Supplanting state, local, territory funds
- Recipient cost-sharing contribution
- Ransom-attack payments
- Any purpose that does not address cybersecurity risks & threats on an information system

MULTISTATE COLLABORATIVE GRANTS

OVERVIEW:

Two or more states may jointly apply for a grant to address cybersecurity risks and threats to information systems within those groups.

FEDERAL-STATE MATCHING REQUIREMENT:

- The federal share of the cost of an activity carried out using the grant funds made available under the program may not exceed: 100% for FY22, 90% for FY23, 80% for FY24, 70% for FY25.
- The state share may not be an in-kind match. This will likely be needed via an appropriation by the state legislature.
- Federal share amounts can be waived or modified if the multistate group demonstrates economic hardship (i.e. changes in unemployment, SNAP eligible individuals and other factors).

NASCIO
Representing Chief Information Officers of the States

REQUIREMENTS:

Each state must:

- Submit a cybersecurity plan that has been reviewed by DHS CISA, describe the divisions of responsibilities and distribution of funding, provided how each state will work together to implement their cybersecurity plan
- Establish a cybersecurity planning committee
- Meet all other requirements/restrictions as a non-multi-state grant

REPORTING REQUIREMENTS:

ANNUAL REPORTS TO DHS CISA:

Within one year after the date the grant was received, the state must provide a report to DHS CISA, which includes:

- Implementation progress of their approved cybersecurity plan
- If no plan exists, how grant funds were obligated and expended to develop a cybersecurity plan or improve information systems
- Annual reports that will be made publicly available and are subject to redactions in order to protect sensitive information.

ANNUAL REPORTS TO CONGRESS:

Each year, DHS CISA must provide a report to Congress, which includes:

- Use of grants awarded and the proportion of grants used to support cybersecurity in rural areas
- Achieving objectives set by the homeland security strategy to improve cybersecurity and any necessary modifications
- Progress towards developing, implementing, or revising cybersecurity plans
- Reducing risk & threats to information systems

STUDY OF RISK-BASED FORMULAS:

No later than September 30, 2024, DHS will submit to Congress a study and legislative recommendation on the use of risk-based formulas for appropriating funds, including components that support rural areas, sources of data and information, obstacles, and any other information that would help congress understand progress towards implementation.

For questions, please contact Matt Pincus (mpincus@nascio.org).